This product was created as part of a joint effort between the Federal Bureau of Investigation, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the United States Secret Service.

Fraud Alert – Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses

19 June 2015

FS-ISAC members and federal law enforcement agencies continue to report an increase in wire transfer fraud against U.S. businesses through a scam referred to as "Business E-mail Compromise" (BEC).[a] BEC is a type of payment fraud that involves the compromise of legitimate business e-mail accounts for the purpose of conducting an unauthorized wire transfer. After a business e-mail account is compromised, actors use the compromised account or a spoofed account to send wire transfer instructions. The funds are primarily sent to Asia, but funds have also been sent to other countries all over the world.

Most of the BEC incidents involve the compromise of an e-mail account belonging to a business's CEO/CFO, in order to send an e-mail to an employee with the ability to conduct wire transfers. Additionally, other incidents involve the compromise of a vendor/supplier's e-mail account with the intention of modifying the bank account associated with that vendor/supplier. The latter scheme may also be labeled as vendor fraud and involves a last minute change of the bank and account number for future payments.

In most cases, after the actors compromise the legitimate business e-mail accounts through social engineering or malware, they conduct reconnaissance to review the business's legitimate e-mail communications and travel schedules.

In some instances, actors have auto-forwarded e-mails received by the victim to an e-mail account under their control. This reconnaissance stage lasts until the actor feels comfortable enough to send wire transfer instructions using either the victim's e-mail or a spoofed e-mail account that is controlled by the actor. The difference in the spoofed e-mail account is very subtle and can easily be mistaken for the legitimate business e-mail address.

[a] In January 2015, the Internet Crime Complaint Center posted a public service announcement on Business E-mail Compromise. The document can be found at www.ic3.gov/media/2015/150122.aspx.

Tradecraft

The actors utilize multiple methods to ensure their e-mail communications are successful. In some instances, actors have created rules using the compromised business e-mail account to send all communications associated with the actor's activity to the trash folder or to a hidden folder the victim is unaware of. A common theme in the CEO/CFO scheme is that the actors wait until the CEO/CFO is on official travel before sending wire transfer instructions, making it more likely that the individual would use e-mail for official business and therefore harder to verify the transaction as fraudulent. These requests will sometimes state that the wire transfer is related to urgent or confidential matters and must not be discussed with any other company personnel.

Risk Mitigation

The key to reducing the risk from BEC is to understand the criminals' techniques and deploy effective payment risk mitigation processes. There are various methods to reduce the risk of falling victim to this scam and subsequently executing a fraudulent wire transfer. Some of these methods include:

- Verifying a change in payment instructions to a vendor or supplier by calling to verbally confirm the request (the phone number should not come from the electronic communication, but should instead be taken from a known contact list for that vendor);
- Maintain a file, preferably in non-electronic form, of vendor contact information for those who are authorized to approve changes in payment instructions;
- Limit the number of employees within a business who have the authority to approve and/or conduct wire transfers;
- Use out of band authentication to verify wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a phone Personal Identification Number (PIN) to verify the executive's identity, or sending the executive via text message a one-time code and a phone number to call in order to confirm the wire transfer request;
- When the staff at a victim business is contacted by the bank to verify the wire transfer, the staff should delay the transaction until additional verifications can be performed; and
- Require dual-approval for any wire transfer request involving:
    - A dollar amount over a specific threshold; and/or
    - Trading partners who have not been previously added to a "white list" of approved trading partners to receive wire payments; and/or
    - Any new trading partners; and/or

- New bank and/or account numbers for current trading partners; and/or
- Wire transfers to countries outside of the normal trading patterns.

Incident Reporting

1. The FBI and USSS encourage victims of cyber crime to contact their local FBI or USSS field office, http://www.fbi.gov/contact/fo/fo.htm or http://www.secretservice.gov/field_offices.shtml, or file a complaint online at www.IC3.gov.
2. Timing is critical. If notified immediately, financial institutions and law enforcement can work with you to increase the chance of recovering the stolen funds.
3. When reporting, be prepared to provide a general description of this crime, how it occurred, losses experienced, and Wiring/ACH instructions.
4. The FS-ISAC encourages member institutions to report any observed fraudulent activity through the FS-ISAC submission process on the FS-ISAC portal or by contacting the FS-ISAC SOC. Submission through the FS-ISAC portal can be done anonymously and will assist other members to prevent, detect, and respond to similar attacks and protect their customers.
5. Financial institutions' compliance or anti-money laundering team(s) should submit a Suspicious Activity Report (SAR) utilizing the BEC term to make it easier for law enforcement to track.