IC3 PUBLIC SERVICE ANNOUNCEMENT
FEDERAL BUREAU OF INVESTIGATION

22 January 2015

Alert Number

I-012215-PSA

BUSINESS E-MAIL COMPROMISE

The Business E-mail Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. Formerly known as the Man-in-the-E-mail Scam, the BEC was renamed to focus on the "business angle" of this scam and to avoid confusion with another unrelated scam. The fraudulent wire transfer payments sent to foreign banks may be transferred several times but are quickly dispersed. Asian banks, located in China and Hong Kong, are the most commonly reported ending destination for these fraudulent transfers.

The BEC is a global scam with subjects and victims in many countries. The IC3 has received BEC complaint data from victims in every U.S. state and 45 countries. From 10/01/2013[1] to 12/01/2014, the following statistics are reported:

- *Total U.S. victims: 1198*
- *Total U.S. dollar loss: $179,755,367.08*

- *Total non-U.S. victims: 928*
- *Total non-U.S. dollar loss: $35,217,136.22*

- *Combined victims:* ***2126***
- *Combined dollar loss:* ***$214,972,503.30***

The FBI assesses with high confidence the number of victims and the total dollar loss will continue to increase.

The BEC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and home/vacation rental scams. The victims of these scams are usually U.S. based and may be recruited as unwitting "money mules."[2] The mules receive the fraudulent funds in their personal accounts and are then directed by the subject to quickly transfer the funds using wire transfer services or another bank account, usually outside the U.S. Upon direction, mules may sometimes open business accounts for fake corporations both of which may be incorporated in the true name of the mule.

The "Attorney Check Scam" is another type of fraud that is linked to the BEC scam in the following manner:

- Attorneys are targeted to represent supposed (BEC) litigants in a payment dispute.
- Retainers in the form of checks are sent by (BEC) litigants to the attorney.
- The scam is revealed when either the checks are found to be fraudulent or the (BEC) litigants are contacted.
- While the payment disputes are real, the (BEC) litigants neither contacted nor retained

[1] The IC3 began tracking the BEC scam 10/01/2013.
[2] "money mules" are defined as a person who transfers money illegally on behalf of others.

that attorney for legal assistance.

The victims of the BEC scam range from small to large businesses. These businesses may purchase or supply a variety of goods, such as textiles, furniture, food, and pharmaceuticals. This scam impacts both ends of the supply chain, as both supplies and money can be lost and business relations may be damaged.

It is still largely unknown how victims are selected; however, the subjects monitor and study their selected victims prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocol necessary to perform wire transfers within a specific business environment. Victims may also first receive "phishing" e-mails requesting additional details of the business or individual being targeted (name, travel dates, etc). Some victims reported being a victim of various Scareware or Ransomware cyber intrusions, immediately preceding a BEC scam request.

VERSIONS OF THE BEC SCAM

Based on IC3 complaints and other complaint data received since 2009, there are three main versions of this scam:

Version 1

A business, which often has a long standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request. This particular version has also been referred to as "The Bogus Invoice Scheme," "The Supplier Swindle," and "Invoice Modification Scheme."

Version 2

The e-mail accounts of high-level business executives (CFO, CTO, etc) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular version has also been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Version 3

An employee of a business has his/her personal e-mail hacked. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.

CHARACTERISTICS OF BEC COMPLAINTS

The IC3 has noted the following characteristics of BEC complaints:

- Businesses and personnel using open source e-mail are most targeted.
- Individuals responsible for handling wire transfers within a specific business are targeted.
- Spoofed e-mails very closely mimic a legitimate e-mail request.
- Hacked e-mails often occur with a personal e-mail account.
- Fraudulent e-mail requests for a wire transfer are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request.
- The phrases “code to admin expenses” or “urgent wire transfer” were reported by victims in some of the fraudulent e-mail requests.
- The amount of the fraudulent wire transfer request is business specific; therefore, dollar amounts requested are similar to normal business transaction amounts so as to not raise doubt.
- Fraudulent e-mails received have coincided with business travel dates for executives whose e-mails were spoofed.
- Victims report that IP addresses frequently trace back to free domain registrars.

SUGGESTIONS FOR PROTECTION

The IC3 suggests the following measures to help protect you and your business from becoming victims of the BEC scam:

- Avoid Free Web-Based E-mail: Establish a company web site domain and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and Financial security procedures and 2-step verification processes. For example -
    - Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
    - Digital Signatures: Both entities on either side of transactions should use digital signatures. However, this will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
    - Delete Spam: Immediately delete unsolicited e-mail (spam) from unknown parties. Do NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
    - Forward vs. Reply: Do not use the “Reply” option to respond to any business e-mails. Instead, use the “Forward” option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient’s correct e-mail address is used.

- Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been on a company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.

FILING AN IC3 COMPLAINT

If you believe your businesses is the recipient of a compromised e-mail or is a victim of the BEC scam (regardless of dollar amount), you should file with the IC3 at www.ic3.gov. Please be as descriptive as possible, identify your complaint as "Business Email Compromise" or "BEC" and try to include the following information:

- Header information from e-mail messages
- Identifiers for the perpetrators such as names, e-mail addresses, websites, bank account information (especially where transfers were requested to be sent), and beneficiary names
- Details on how, why, and when you believe you were defrauded
- Actual and attempted loss amounts
- Other relevant information you believe is necessary to support your complaint

Complainants are also encouraged to keep all original documentation, e-mails, faxes, and logs of all telecommunications. You will not be able to add or upload attachments with your IC3 complaint; however, please retain all relevant information, in the event you are contacted by law enforcement.

FILING A SUSPICIOUS ACTIVITY REPORT (SAR)

Financial Institutions which file a SAR related to the BEC scam are requested to aid in the following:

- Refer to the scam as "Business E-mail Compromise."
- Identify all victims of the BEC scam to include by name and descriptive data not only the business sending the fraudulent transfer but also their suppliers (as applicable), employee names whose identities were stolen and used to establish fraudulent accounts, and any other financial institutions involved.
- Provide as much victim detail as possible to include the following:
    - Full name and address of all businesses, suppliers, and individuals
    - All available bank account information for the account *receiving* the fraudulent transfers, such as bank name and address, account numbers involved, and beneficiary account information, including Personally Identifiable Information (PII) if available.