Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 14, 2016

Alert Number

I-061416-PSA

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

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

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

DEFINITION

BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

STATISTICAL DATA

The BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300% increase in identified exposed losses[1]. The scam has been reported by victims in all 50 states and in 100 countries. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to Asian banks located within China and Hong Kong.

The following BEC statistics were reported to the IC3 and are derived from multiple sources to include IC3 victim complaints and complaints filed with international law enforcement agencies and financial institutions:

Domestic and International victims: 22,143
Combined exposed dollar loss: $3,086,250,090

The following BEC statistics were reported in victim complaints to the IC3 from October 2013 to May 2016:

Domestic and International victims: 15,668
Combined exposed dollar loss: $1,053,849,635

- *Total U.S. victims: 14,032*
- *Total U.S. exposed dollar loss: $960,708,616*
- *Total non-U.S. victims: 1,636*
- *Total non-U.S. exposed dollar loss: $93,141,019*

[1] Exposed dollar loss includes actual and attempted loss in United States dollars.

BACKGROUND
The victims of the BEC scam range from small businesses to large corporations. The victims continue to deal in a wide variety of goods and services, indicating a specific sector does not seem to be targeted.

It is largely unknown how victims are selected; however, the subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment. Victims may also first receive "phishing" e-mails requesting additional details regarding the business or individual being targeted (name, travel dates, etc.).

Some individuals reported being a victim of various Scareware or Ransomware cyber intrusions immediately preceding a BEC incident. These intrusions can initially be facilitated through a phishing scam in which a victim receives an e-mail from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the actor(s) unfettered access to the victim's data, including passwords or financial account information.

The BEC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and 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 to another bank account, usually outside the U.S. Upon direction, mules may open bank accounts and/or shell corporations to further the fraud scheme.

SCENARIOS OF BEC
Based on IC3 complaints and other complaint data[3] , there are five main scenarios by which this scam is perpetrated. BEC victims recently reported a new scenario (Data Theft) involving the receipt of fraudulent e-mails requesting either all Wage or Tax Statement (W-2) forms or a company list of Personally Identifiable Information (PII). This scenario does not always involve the request for a wire transfer; however, the business executive's e-mail is compromised, either spoofed or hacked, and the victims are targeted in a similar manner as described in Scenario 2 of the BEC scam.

Scenario 5 (New): Data Theft

Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entity in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipient of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario, even if they were able to successfully identify and avoid the traditional BEC incident. The data theft scenario (Scenario 5) of the BEC first appeared just prior to the 2016 tax season.

[2] Money mules are defined as persons who transfer money illegally on behalf of others.
[3] Multiple source complaint data, not limited to IC3, describing the BEC scam is dated as far back as 2009.

Scenario 1: Business Working With a Foreign Supplier
A business, which often has a long standing relationship with a supplier, is requested 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 scenario has also been referred to as "The Bogus Invoice Scheme," "The Supplier Swindle," and "Invoice Modification Scheme."

Scenario 2: Business [Executive] Receiving or Initiating a Request for a Wire Transfer
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 scenario has also been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail
An employee of a business has his/her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. 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 that business is contacted by a vendor to follow up on the status of an invoice payment.

Scenario 4: Business Executive and Attorney Impersonation
Victims report being contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

CHARACTERISTICS OF BEC COMPLAINTS
The IC3 has noted the following characteristics of BEC complaints:

- Businesses and associated personnel using open source e-mail accounts are predominantly 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 and BEST PRACTICES
Businesses with an increased awareness and understanding of the BEC scam are more likely to recognize when they have been targeted by BEC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.

Businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting BEC attempts.

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.

The following is a compilation of self protection strategies provided in the BEC PSAs from 2015.

- Avoid free web-based e-mail accounts: Establish a company domain name 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, including the implementation of a 2-step verification process. 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 each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
    - Delete Spam: Immediately report and 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.
    - Consider implementing Two Factor Authentication (TFA) for corporate e-mail accounts. TFA mitigates the threat of a subject gaining access to an employee’s e-mail account through a compromised password by requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code).

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

through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of *abc_company.com* would flag fraudulent e-mail of *abc-company.com*.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

Additional information is publicly available on the United States Department of Justice website www.justice.gov publication entitled "Best Practices for Victim Response and Reporting of Cyber Incidents".

WHAT TO DO IF YOU ARE A VICTIM

If funds are transferred to a fraudulent account, it is important to act quickly:

- Contact your financial institution immediately upon discovering the fraudulent transfer
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds
- File a complaint, regardless of dollar loss, at www.IC3.gov

When contacting law enforcement or filing a complaint with the IC3, it is important to identify your incident as "BEC", provide a brief description of the incident, and consider providing the following financial information:

- Originating[4] Name:
- Originating Location:
- Originating Bank Name:
- Originating Bank Account Number:
- Recipient[5] Name:
- Recipient Bank Name:
- Recipient Bank Account Number:
- Recipient Bank Location (if available):
- Intermediary Bank Name (if available):
- SWIFT Number:
- Date:

[4] The term "Originating" is synonymous with the term "Victim"
[5] The term "Recipient" is synonymous with the term "Beneficiary"

- Amount of Transaction:
- Additional Information (if available) - including “FFC”- For Further Credit; “FAV” – In Favor Of:

FILING A COMPLAINT WITH IC3

Victims should always file a complaint regardless of dollar loss or timing of incident at www.IC3.gov and, in addition to the financial information, provide the following descriptors:

- IP and/or e-mail address of fraudulent e-mail
- Date and time of incidents
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Phone numbers of the fraudulent phone calls
- Description of any phone contact to include frequency and timing of calls
- Foreign accents of the callers
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity