$3.1 BILLION SCAM – HIJACKED E-MAIL ACCOUNTS INVITE WIRE TRANSFER FRAUD

Author
Simon H. Prisk

Tags
Business E-mail Compromise
E-mail Hacking
Internet Crime Complaint Center ("IC3")
Wire Fraud

The Federal Bureau of Investigation ("F.B.I.") released a public service announcement ("P.S.A.") regarding what is known as the Business E-mail Compromise ("B.E.C."), a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.[1]

The B.E.C. scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques in order to conduct unauthorized transfers of funds. Most victims report using wire transfers as a common method of transferring funds for business purposes, although some victims also report using checks. The digital thieves use the method most commonly associated with their victims' normal business practices.

STATISTICAL DATA

The B.E.C. 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.[2]

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 in China and Hong Kong.

Combined Reporting

The following B.E.C. statistics were reported to the Internet Crime Complaint Center ("IC3") and are derived from multiple sources, including 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

IC3 Victim Complaints

The following B.E.C. statistics are derived from victim complaints to the IC3, in the period from October 2013 to May 2016:

---

1 The article reproduces much of the information printed in F.B.I. alert no. I-061416-PSA, which can be seen online here.

2 Exposed dollar loss includes actual and attempted loss in U.S. dollars.

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. Dollar Exposed Loss:	$93,141,019

BACKGROUND

The victims of the B.E.C. scam range from small businesses to large corporations. Victims deal in a wide variety of goods and services, indicating that a specific sector does not seem to be targeted.

It is largely unknown how victims are selected. However, it is known that the subjects monitor and study their selected victims using social engineering techniques prior to initiating the B.E.C. 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 (*e.g.*, name, travel dates, etc.).

Some individuals reported being a victim of various Scareware or Ransomware cyber intrusions immediately preceding a B.E.C. 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, which downloads malware, allowing the actor(s) unfettered access to the victim's data, including passwords or financial account information.

The B.E.C. 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.[3] 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 B.E.C.

Based on IC3 complaints and other complaint data,[4] there are five main scenarios by which the B.E.C. scam is perpetrated.

---

[3] Money mules are persons who transfer money illegally on behalf of others.

[4] Multiple source complaint data, not limited to IC3, describing the B.E.C. scam is dated as far back as 2009.

"The B.E.C. scam is linked to other forms of fraud, including but not limited to romance, lottery, employment, and rental scams."

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 the "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 (*e.g.*, C.F.O., C.T.O., 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 "C.E.O. Fraud," the "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 or her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. Requests for invoice payments to bank accounts controlled by a digital thief are sent from the employee's personal e-mail address to multiple vendors identified from the employee's contact list. The business may not become aware of the fraudulent requests until the 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 digital thieves, 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 digital thief to act quickly or secretly in handling the transfer of funds. This type of B.E.C. 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.

Scenario 5: Data Theft

B.E.C. victims recently reported a new scenario 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 ("P.I.I."). 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 B.E.C. scam. Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entity in the business

organization responsible for W-2's or maintaining P.I.I., 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's and/or P.I.I. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new B.E.C. scenario, even if they were able to successfully identify and avoid the traditional B.E.C. incident. The data theft scenario of the B.E.C. first appeared just prior to the 2016 tax season.

CHARACTERISTICS OF B.E.C. COMPLAINTS

The IC3 has noted the following characteristics of B.E.C. complaints:

- Targets are predominantly businesses and associated personnel using open source e-mail accounts.
- 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 as to the legitimacy of the request.
- The phrase "code to admin expenses" or "urgent wire transfer" was 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 I.P. addresses frequently trace back to free domain registrars.

"Targets are predominantly businesses and associated personnel using open source e-mail accounts."

SUGGESTIONS FOR PROTECTION AND BEST PRACTICES

Businesses with an increased awareness and understanding of the B.E.C. scam are more likely to recognize when they have been targeted by B.E.C. digital thieves, 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 frontline employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting B.E.C. 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 B.E.C. P.S.A.'s from 2015.[5]

- 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 about what is posted to social media and company websites, especially job duties or descriptions, hierarchal information, and out-of-office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional I.T. and financial security procedures, including the implementation of a two-step verification process.
    - 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 v. 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 ("T.F.A.") for Corporate E-mail Accounts: T.F.A. 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: (i) something the user knows (a password) and (ii) something the user has (such as a dynamic P.I.N. or code).
- 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 domain names that are similar to the company's e-mail domain. For example, where the legitimate domain name of an e-mail address is abc_company.com, the system

[5] Additional information is publicly available in the U.S. Department of Justice website, www.justice.gov, publication entitled "Best Practices for Victim Response and Reporting of Cyber Incidents."

would flag a fraudulent e-mail from 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 T.F.A., such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of the T.F.A., 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.

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 F.B.I. office if the wire is recent. The F.B.I., working with the U.S. Department of Treasury Financial Crimes Enforcement Network ("FinCEN"), might be able to help return or freeze the funds.
- File a complaint, regardless of dollar loss, with the IC3.

"Victims should always file a complaint with the IC3 regardless of the dollar loss or timing of the incident."

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

- Originating[6] name
- Originating location
- Originating bank name
- Originating bank account number
- Recipient[7] name
- Recipient bank name
- Recipient bank account number
- Recipient bank location (if available)

---

[6] The term "originating" is synonymous with the term "victim."

[7] The term "recipient" is synonymous with the term "beneficiary."

- Intermediary bank name (if available)
- S.W.I.F.T. number
- Date
- Amount of transaction
- Additional information, if available, including F.F.C. (for further credit) and F.A.V. (in favor of)

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

- I.P. 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

Complaints may be filed with the IC3 online at www.IC3.gov.