Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 July 2016

PIN Number

160721-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:

www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:

1-855-292-3937

Cyber Criminals Using Business E-mail Compromise Schemes to Steal Millions of Dollars from US Companies

Summary

Business E-mail Compromise (BEC) is 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 wire transfers. Victim reporting indicates a vast majority of the fraudulent wire transfers initiated through BEC schemes are destined for banks in Mainland China and Hong Kong.

Technical Details

While it is unclear how victims are selected, cyber criminals are known to monitor and study their selected victims prior to initiating the BEC scam, and are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment. Some actors may also first send phishing e-mails requesting additional details on the business or individual being targeted, such as names and business travel dates of corporate personnel, to gain additional insight into the company and increase the perceived credibility of the scheme. Three of the most common BEC schemes include the compromise of e-mail accounts belonging to:

1. Business Executives: An e-mail account belonging to a business executive with the authority to request wire transfers, such as a CEO or CFO, is compromised and subsequently used to send wire transfer instructions to an employee with the ability to conduct wire transfers. Cyber criminals will commonly wait until the executive is out of the office on travel before sending

wire transfer instructions, making the executive's use of e-mail for official business communications more realistic and simultaneously increasing the difficulty of identifying the transaction as fraudulent.

2. Vendors: An e-mail account belonging to a vendor that receives payments through wire transfers is compromised and subsequently used to send messages to clients, instructing them to send all future wire transfers to a new bank account that is under the cyber criminal's control. As the actual wire transfer requests and payments remain legitimate, the fraud may be harder to detect until the vendor inquires about the missing payments.
3. Employees: A personal e-mail account belonging to an employee that sends invoice payment requests is compromised and subsequently used to send instructions to vendors identified through the employee's contact list requesting payments be made to accounts under the cyber criminal's control.

Threat

The FBI tracked a total of 44 fraudulent wire transfers provided through victim reporting that occurred as a result of BEC between 9 December 2015 and 9 March 2016 totaling $75,657,487. The wire transfers averaged approximately $1.7 million, and the largest attempted wire transfer was over $19.8 million. Most of these BEC incidents involved the compromise of an e-mail account belonging to a CEO/CFO and the subsequent use of that account to e-mail wire transfer instructions to an employee with the ability to conduct wire transfers.

Cyber criminals primarily deceived victims into sending funds to beneficiary accounts in Hong Kong and Mainland China, accounting for 31 of the 44 transactions and approximately 84 percent of the stolen funds. 56 percent of the fraudulent wire transfers sent to Hong Kong were sent to beneficiary accounts at The Hongkong [sic] and Shanghai Banking Corporation (HSBC) while beneficiary accounts at Hang Seng Bank received the second most at only 17 percent. Beneficiary accounts located in Hong Kong and Mainland China exacerbates the BEC threat due to limited opportunities to deter actors and restore stolen funds to victims.

For a more comprehensive description of BEC schemes and additional BEC loss statistics, see Public Service Announcement (PSA) I-061416-PSA on www.ic3.gov.

Defense

Precautionary measures to prevent falling victim to BEC schemes include:

- Carefully scrutinize all e-mail requests for wire transfers to determine if the requests are out of the ordinary.
- Confirm wire transfer instructions with the requester, especially when the requester is out of the office, using an alternate and previously established communication avenue to avoid the fraudster receiving and spoofing the confirmation request.
- Require multiple approval authorities, and establish this procedure in such a way that would be difficult for fraudsters to discover.
- Question any variations to typical business practices and wire transfer activity, such as a current business contact suddenly asking to be contacted via their personal e-mail address when all previous official correspondence has been through a company e-mail address.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Scrutinize e-mail addresses for accuracy and be aware of small changes that mimic legitimate addresses, such as single characters that have been added, removed, or duplicated in the local segment of the address, or a change in the hostname.
    - Local Example: “username@abc.com” vs. “userrname@abc.com”
    - Hostname Example: “username@abc.com” vs. “username@def.com”
- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail extensions.
    - Example: “abc_company” vs. “abc-company”
- Register all company domains that are slightly different than the actual company domain.
- Use discretion when posting to social media and company Web sites, especially job duties/descriptions, hierarchal information, and out-of-office details.

What to do if you are a victim:

If funds are transferred to a criminal account, it is imperative 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 FBI office. The FBI, working with the United States 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 www.bec.ic3.gov.

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

- Originating[a] business name
- Originating financial institution name and address
- Originating account number
- Recipient[b] name
- Recipient financial institution name and address
- Recipient account number
- Correspondent bank if known or applicable
- Dates and amounts transferred
- IP and/or e-mail address of fraudulent e-mail
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity
- Description of any phone contact, including frequency and timing of calls
- Phone numbers of the fraudulent phone calls
- Foreign accents of the callers

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report

[a] The term "Originating" is synonymous with the term "Victim."
[b] The term "Recipient" is synonymous with the term "Beneficiary."

submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey