Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

August 27, 2015

Alert Number
I-082715a-PSA

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

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

BUSINESS EMAIL COMPROMISE

This Public Service Announcement (PSA) is an update for the Business E-mail Compromise (BEC) PSA I-012215-PSA posted on www.IC3.gov and includes new information and updated statistical data as of August 2015.

DEFINITION

Business Email Compromise (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.[1]

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 and evolve and it targets businesses of all sizes. There has been a 270 percent increase in identified victims and exposed loss since January 2015. The scam has been reported in all 50 states and in 79 countries. Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong.

The following BEC statistics were reported to the Internet Crime Complaint Center from **October 2013 to August 2015:**

- Total U.S. Victims: 7,066
- Total U.S. exposed[2] dollar loss: $747,659,840.63
- Total non-U.S. victims: 1,113
- Total non-U.S. exposed dollar loss: $51,238,118.62
- Combined victims: 8,179
- Combined exposed dollar loss: $798,897,959.25

These totals, combined with those identified by international law enforcement agencies during this same time period, bring the BEC exposed loss to over $1.2 billion.

RECENT TRENDS

There has been an increase in the number of reported computer intrusions linked to BEC scams. 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.

Three versions of the BEC scam were described in PSA I-012215-PSA. A fourth version of this scam has recently been identified, based on victim complaints.

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 or be timed to coincide with the close of business of international financial institutions.

SUGGESTIONS FOR PROTECTION

Raised awareness of the BEC scam has helped businesses detect the scam before sending payments to the fraudsters. 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.

Businesses reported using the following new measures for added protection:

- 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 transfer 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, with www.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 business name
- Originating financial institution name and address
- Originating account number
- Beneficiary name
- Beneficiary financial institution name and address
- Beneficiary account number
- Correspondent bank if known or applicable
- Dates and amounts transferred
- IP and/or e-mail address of fraudulent e-mail

Detailed descriptions of BEC incidents should include but not be limited to the following when contacting law enforcement:

	• 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, including 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 1.This definition was revised to emphasize the different techniques used to compromise victim e-mail accounts. ↩ 2.Exposed dollar loss includes actual and attempted loss in United States dollars. ↩