Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

10 September 2019

Alert Number
I-091019-PSA

BUSINESS EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.[1]

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses[2]. The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.

Based on the financial data, banks located in China and Hong Kong remain the primary destinations of fraudulent funds. However, the Federal Bureau of Investigation has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and July 2019**:

Domestic and international incidents: 166,349
Domestic and international exposed dollar loss: $26,201,775,589

[1] Reference PSA 1-022118-PSA Increase in W-2 Phishing Campaigns
[2] Exposed dollar loss includes actual and attempted loss in United States dollars

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and July 2019**:

Total U.S. victims: 69,384
Total U.S. exposed dollar loss: $10,135,319,091

Total non-U.S. victims: 3,624
Total non-U.S. exposed dollar loss: $1,053,331,166

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019**:

Total U.S. financial recipients: 32,367
Total U.S. financial recipient exposed dollar loss: $3,543,308,220

Total non-U.S. financial recipients: 14,719
Total non-U.S. financial recipient exposed dollar loss: $4,843,767,489

BEC AND PAYROLL DIVERSION

The IC3 has received an increased number of BEC complaints concerning the diversion of payroll funds. Complaints indicate that a company's human resources or payroll department receives spoofed emails appearing to be from employees requesting a change to their direct deposit account. This is different from the payroll diversion scheme in which the subject gains access to an employee's direct deposit account and alters the routing to another account.[3]

In a typical example, HR or payroll representatives received emails appearing to be from employees requesting to update their direct deposit information for the current pay period. The new direct deposit information provided to HR or payroll representatives generally leads to a pre-paid card account.

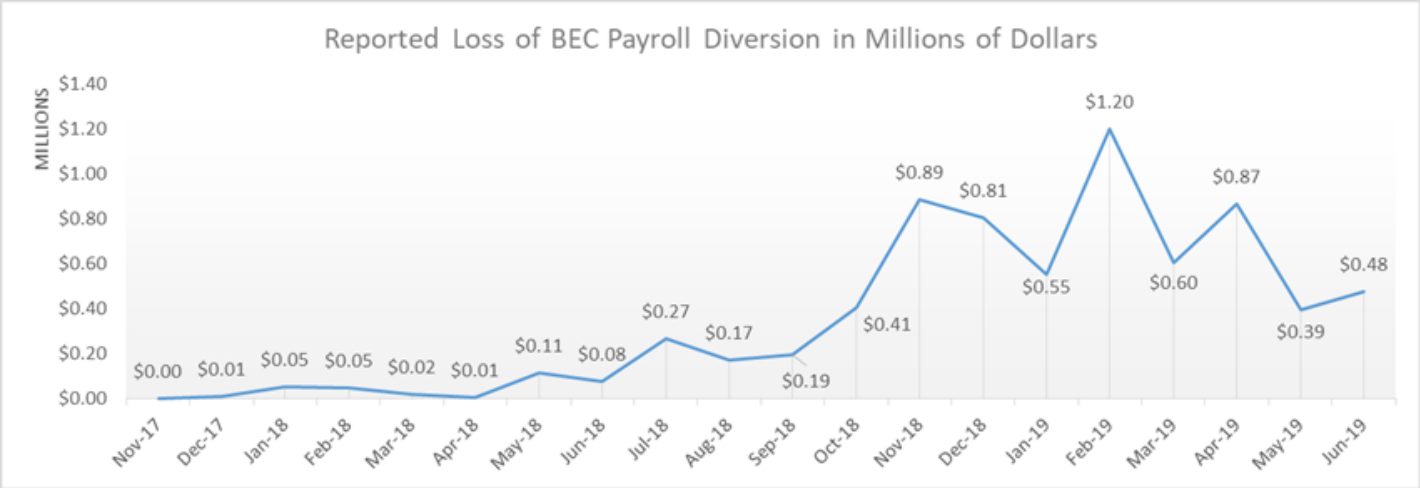
Some companies reported receiving phishing emails prior to receiving requests for changes to direct deposit accounts. In these cases, multiple employees may receive the same email that contains a spoofed log-in page for an email host. Employees enter their usernames and passwords on the spoofed log-in page, which allows the subject to gather and use employee credentials to access the employees' personal information. This makes the direct deposit requests appear legitimate.

Payroll diversion schemes that include an intrusion event have been reported to the IC3 for several years. Only recently, however, have these schemes been directly connected to BEC actors through IC3 complaints.

A total of 1,053 complaints reporting this BEC evolution of the payroll diversion scheme were filed with the IC3 between Jan. 1, 2018, and June 30, 2019, with a total reported loss of $8,323,354. The average dollar loss reported in a

[3] Reference PSA I-091818-PSA Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion

complaint was $7,904. The dollar loss of direct deposit change requests increased more than 815 percent between Jan. 1, 2018, and June 30, 2019 as there was minimal reporting of this scheme in IC3 complaints prior to January 2018.



SUGGESTIONS FOR PROTECTION

Employees should be educated about and alert to this scheme. Training should include preventative strategies and reactive measures in case they are victimized. Among other steps, employees should be told to:

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII in response to any emails.
- Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits.
- Keep all software patches on and all systems updated.
- Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the senders address email address appears to match who it is coming from.
- Ensure the settings the employees' computer are enabled to allow full email extensions to be viewed.

If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds and your employer to report irregularities with payroll deposits.

As soon as possible, file a complaint regardless of the amount with www.ic3.gov or, for BEC/EAC victims, BEC.IC3.gov.