Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

03 August 2018

PIN Number

180803-001

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@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP: Green: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion

This notification was created jointly by the FBI and the National Cyber Forensics & Training Alliance (NCFTA).

Summary

The FBI has observed an increase in cybercriminal actors using widespread tactics to gain access to companies' employee payroll data. In 2017, the FBI and IC3 identified approximately 17 cases. As of July 2018, the FBI and IC3 have identified approximately 47 payroll diversion cases, with losses totaling approximately $1million. Various institutions most affected by the outcomes of this cyber focused scheme include but are not limited to: universities, local school districts, healthcare, and commercial airway transportation. The FBI has observed two main social engineering methods in which the cybercriminal actors gain access to and alter employees' information, either via online phishing email or through telephone solicitation.

Methodologies

Cyber criminals use Payroll Diversion to obtain credentials from victim companies, utilizing the login credentials of employees to access payroll

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607

portals and reroute direct deposits to fraudulent accounts owned by the actors. Cybercriminal actors divert payroll funds to prepaid bank cards which are controlled by the actors. Often the fraudulent payroll deposits arrive from multiple victims' accounts into the cybercriminal controlled accounts.

For the first observed social engineering method, victim credentials are targeted with a customized email that contains either a link to a phishing website or a .pdf file that redirects the user to the phishing site. In most cases, this phishing site is made to look like the legitimate HR software service the victim company provides. The victim is prompted to enter their login credentials which are captured by the actor. The actor logs into the employee's account and changes the bank account information to an account controlled by the actor. When the next deposit is made, the funds are routed to the actor as opposed to the employee's account.

The second observed social engineering method involves the cybercriminal actor calling the employees' resource hotline and providing the employee ID number and last four numbers of the Social Security number to reset the victim's password.

NCFTA intelligence analysts reviewed transactional data related to this activity and determined there were a total of approximately 205 fraudulent payroll deposits made to the pre-paid cards. In addition, the average time frame between when a card is activated and used to receive the fraudulent direct deposits is 54 days, with the minimum being one day. The cybercriminal actors tend to use the bank cards to receive cash withdrawals from ATM machines, or make purchases at gas stations, grocery stores, retail stores, fast food restaurants, and wireless phone carrier providers.

Recommendations

To mitigate the threat of payroll diversion:

- Alert your workforce to this scheme.
- Apply heightened scrutiny to bank information initiated by the employees seeking to update or change direct deposit credentials.
- Educate personnel on appropriate preventative and reactive actions to known criminal schemes and social engineering threats.
- Instruct employees to refrain from supplying log-in credentials or personally identifying information in response to any email.
- Direct employees to forward any suspicious requests for personal information to the information technology or human resources department.

- Ensure that log-in credentials used for payroll purposes differ from those used for other purposes, such as employee surveys.
- Monitor employee logins that occur outside of normal business hours.
- Restrict access to the Internet on systems handling sensitive information.
- Implement two-factor authentication for access to sensitive systems and information.
- Only allow required processes to run on systems handling sensitive information.

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 ww.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by email at CyWatch@fbi.gov. When available, each report 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

For comments or questions related to the content or dissemination of this product, contact CyWatch.

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

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.

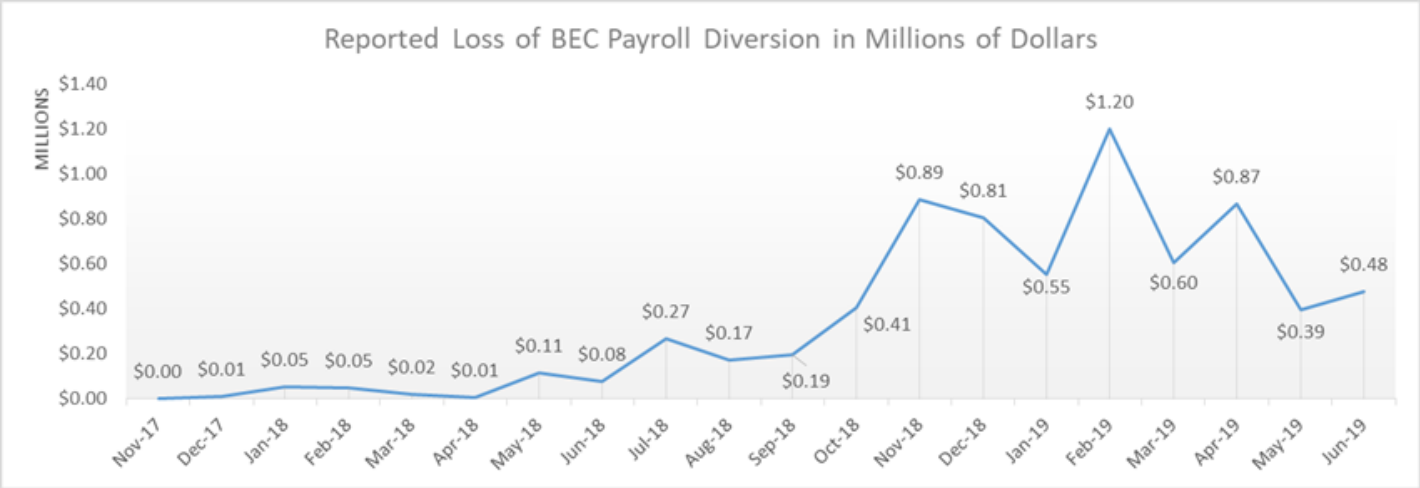
Some companies reported receiving phishing emails prior to receiving requests for changes to direct deposit accounts. In these cases, multiple employees may receive the same email that contains a spoofed log-in page for an email host. Employees enter their usernames and passwords on the spoofed log-in 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.