Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 July 2018

PIN Number
180719-001

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 in order 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.

BEC Actors Conduct Reconnaissance by Phone to Increase Effectiveness of Campaigns

Summary

Recent FBI reporting indicates cyber criminals have begun contacting potential fraud victims directly via telephone under false pretenses to obtain information (such as names, email addresses, and phone numbers) to increase the effectiveness of subsequent Business Email Compromise (BEC) activity. Cyber criminals may impersonate customers or clients to obtain non-sensitive information, such as employee names and contact information. Such information allows perpetrators to compose personalized malicious emails targeting a person or company. Further, the phone calls can enable the cyber criminals to determine the non-public contact information of individuals within companies who may fall victim to BEC-related activities. This may help bypass established procedures implemented to flag suspicious electronic communications.

- As an example, BEC perpetrators may contact a company's help line and use social engineering to obtain names or contact information of employees or executives. Such information facilitates attempts to hack or spoof email addresses as part of a typical BEC scheme.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

BEC schemes have cost US victims more than $ 3.6 billion in fraud losses over the last five years. This activity is a pervasive threat with significant financial losses and a considerable global impact, based upon victim reports and information from international law enforcement agencies.

Recommendations:

The following list includes precautionary measures and mitigation strategies for BEC threats:

- Conduct end user education and training on the BEC threat and spear phishing emails; Update training to reflect the threat of reconnaissance by phone
- Monitor what information is available on the company's phone lines as well as public-facing websites and social media accounts
- Frequently monitor your email exchange server for changes in configuration and custom rules for specific accounts
- Consider adding an email banner stating when an email comes from outside your organization, so that it is easily noticed
- Ensure company policies provide verification of any changes to existing invoices, bank deposit information, and contact information
- Contact requestors by phone before complying with email requests for payments or personnel records
- Consider requiring two party sign off on payment transfers

The following list includes precautionary measures and mitigation strategies for phone scams:

- Verify the source of the phone call from a list of approved vendors or by calling the public access number of government agencies
- Do not provide payment information over the phone
- Be suspicious of requests for secrecy or pressure to take action quickly
- Be suspicious of requests for abnormal payment methods, such as through a gift card

How and What to Report

The FBI requests BEC victims file a complaint with IC3, regardless of dollar loss or timing of incident. IC3 complaints should be filed at www.IC3.gov with the following details (if applicable):

- Any messages pertaining to the attack. Save correspondence in its original, un-forwarded format
- Victim Information
- Overall losses associated with the BEC
- If a payment associated with the attack was sent, provide transaction details
- Victim impact statement (e.g., impacted services/operations)
- IP addresses used to send fraudulent emails

This product is marked **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

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