Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 March 2019

PIN Number
20190313-001

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

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.

Fraudulent Purchase Order Scams Targeted Defense Industrial Base Sector and Academic Institutions

Summary

The FBI has identified recent business e-mail compromise (BEC) scams where unknown individual(s), posing as legitimate employees of cleared defense contractors (CDC) as well as an academic institution, obtained fraudulent lines of credit, and subsequently acquired high-end technical merchandise. Financial losses from these scams ranged in the tens of thousands of dollars and could have been mitigated by having a process in place where suppliers contacted purchasers and confirmed email address domain names and/or shipping addresses; or placed a hold on a shipment until a purchaser could be reached by phone. Cyber criminals were able to exploit supply companies by purchasing high-value merchandise without suspicion by portraying CDCs and academic institutions.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

BEC / Fraudulent Purchase Order Scams Resulting in Financial Loss for US Companies

In 2018, cyber criminals impersonated at least three CDCs, as well as an academic institution, while obtaining fraudulent lines of credit and acquiring very expensive, high-end technical merchandise. Using obfuscated CDC email addresses, the perpetrator(s) requested product quotes online, communicated with suppliers, and sent fraudulent purchase orders and credit documents, including shipping addresses of warehouses or freight-forwarding companies located in the US. Following shipment of the high-end technical merchandise, the supplier billed the legitimate CDC or academic institution, resulting in financial losses totaling at least tens of thousands of dollars. If successful at placing an order, the perpetrator(s) placed a second larger order several days after the first.

In March 2018, after being notified by multiple suppliers, a CDC realized it was a victim of a BEC scam once it was placed on multiple selling holds for non-payment of the purchases. A few months later, another CDC reported three separate fraudulent orders involving the purchase of laptops and technological equipment. The financial losses to these two CDCs totaled more than $50,000 and $40,000, respectively. Between March and August 2018, a third CDC reported seven attempts to fraudulently order high-end technological or scientific merchandise, which, if gone undetected, could have exceeded $250,000. A similar BEC scam in June 2018 involved fraudulent purchases from a Department of Defense (DoD) supplier. An individual impersonating a legitimate employee from a large university placed two orders for 150 digital multimeters from the DoD supplier, resulting in a loss of approximately $80,000.

Indicators[a] of BEC / Fraudulent Purchase Attempts

Suppliers should be particularly alert to unknown company representatives submitting quote requests via the supplier's website, without the purchasers' subsequent acknowledgment or without validating through any existing corporate relationships. If the paperwork electronically submitted by a purchaser contains errors or misspellings, identifying information is omitted, or the purchaser's email address is inconsistent with

[a] While an indicator alone doesn't accurately determine a scam, the totality of behavior, message delivery, and other relevant circumstances should be evaluated when considering notification of security/law enforcement personnel.

the company's official web address, suppliers should be concerned about a BEC scam. Another indicator of a fraudulent electronic purchase attempt is if the purchaser will only communicate via e-mail, even if a telephone number is provided. Finally, if the shipping destination for an on-line order is a new address, or is not an address publicly associated with the purchasing company, suppliers should be alerted to a possible BEC scam.

Recommendations for Protecting Your Company from BEC Fraud

Purchasing companies can increase their BEC defenses by establishing written policies requiring two parties to sign off on payment transfers, including specific provisions for verifying and validating any changes to existing invoices, bank deposit information, and/or customer and bank contact information. Another recommended two-factor authentication defense policy requires purchasers to contact suppliers by phone prior to having suppliers comply with email requests for payments or personnel records.

If your company is a victim and/or you have knowledge of a potential BEC incident, report it to your security office, the originating bank, your local FBI Field Office, www.fbi.gov/contact-us/field, and the Internet Crimes Complaint Center (IC3), www.ic3.gov.BEC. It is important to include the following details in any reported BEC complaint:

- Victim Information
  - Impact statement (e.g., impacted services/operations)
  - Overall losses associated with the BEC

- Any email messages pertaining to the attack
  - Save correspondence in its original (unforwarded) format
  - If a payment associated with the attack was sent, provide transaction details
  - IP addresses used to send fraudulent emails

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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 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

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