JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA22-340A

December 15, 2022

Criminal Actors Use Business Email Compromise to Steal Large Shipments of Food Products and Ingredients

SUMMARY

The Federal Bureau of Investigation (FBI), the Food and Drug Administration Office of Criminal Investigations (FDA OCI), and the US Department of Agriculture (USDA) are releasing this joint Cybersecurity Advisory (CSA) to advise the Food & Agriculture sector about recently observed incidents of criminal actors using business email compromise (BEC) to steal shipments of food products and ingredients valued at hundreds of thousands of dollars.

Immediate Actions Businesses Can Take Now to Protect Against Product Theft and BEC Schemes:

- Train employees on how to identify fraudulent email addresses and domains.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- Conduct web searches for your company name to identify fraudulent websites that may be used to impersonate you in a scam.

While BEC is most commonly used to steal money, in cases like this criminals spoof emails and domains to impersonate employees of legitimate companies to order food products. The victim company fulfills the order and ships the goods, but the criminals do not pay for the products. Criminals may repackage stolen products for individual sale without regard for food safety regulations and sanitation practices, risking contamination or omitting necessary information about ingredients, allergens, or expiration dates. Counterfeit goods of lesser quality can damage a company's reputation.

BEC is one of the most financially damaging online crimes. According to the FBI's Internet Crime Complaint Center, victims reported losses of almost $2.4 billion in 2021, based on 19,954 recorded complaints linked to BEC attacks targeting individuals and businesses. This CSA provides mitigation

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices, or file a report at IC3.gov. Contact the FDA Office of Criminal Investigations to report suspected criminal activity relating to FDA regulated products at FDA OCI.

recommendations to help reduce the risk of financial loss and possible food contamination resulting from these schemes.

THREAT OVERVIEW

Tactics, Techniques, and Procedures

Threat actors may target Food & Agriculture businesses using the following common tactics, techniques, and procedures (TTPs) to steal food products and ingredients:

- Creating email accounts and websites that closely mimic those of a legitimate company. The accounts and web addresses may include extra letters or words, substitute characters (such as the number "1" for a lower case "l"), or use a different top level domain (such as *.org* instead of *.gov*).
- Gaining access to a legitimate company's email system to send fraudulent emails. Spear phishing is one of the most prevalent techniques used for initial access to IT networks; personnel may open malicious attachments or links contained in emails from threat actors to execute malicious payloads that allow access to the network.
- Adding legitimacy to the scam by using the names of actual officers or employees of a legitimate business to communicate with the victim company.
- Copying company logos to lend authenticity to their fraudulent emails and documents.
- Deceiving the victim company into extending credit by falsifying a credit application. The scammer provides the actual information of a legitimate company so the credit check results in an approval of the application. The victim company ships the product but never receives payment.

Food & Agriculture Sector BEC Incidents

In recent incidents, criminal actors have targeted physical goods rather than wire transfers using BEC tactics. Companies in all sectors—both buyers and suppliers—should consider taking steps to protect their brand and reputation from scammers who use their name, image, and likeness to commit fraud and steal products.

Recent BEC incidents targeting the Food & Agriculture sector include:

- In August 2022, a US sugar supplier received a request through their web portal for a full truckload of sugar to be purchased on credit. The request contained grammatical errors and purportedly came from a senior officer of a US non-food company. The sugar supplier identified the email address had an extra letter in the domain name and independently contacted the actual company to verify there was no employee by that name working there.
- In August 2022, a food distributor received an email purportedly from a multinational snack food and beverage company requesting two full truckloads of powdered milk. The criminal actor used the real name of the chief financial officer of the snack food company but used an email address containing an extra letter in the domain name. The victim company had to pay their supplier more than $160,000 for the shipment after responding to the fraudulent request.

- From at least June through August 2022, unknown criminal actors used the identity of a US company to fraudulently attempt to obtain store credit and/or place large purchase orders to procure shipments of powdered milk and other ingredients from multiple suppliers. Industry dairy vendors notified the company that the unknown third party created falsified credit applications, purchase orders, and invoices in their attempts to place large orders for powdered milk. In one instance, the attempted purchase orders totaled nearly $230,000. In another instance, a vendor shipped two truckloads of powdered milk valued at approximately $200,000. The criminal actors sent emails using the names of the victim company's president and other employees, used the company's logo, a variation of the company's name, and an email address that varied only slightly from real company addresses.
- In April 2022, a US food manufacturer and supplier received a request through their web portal inquiring about pricing for whole milk powder purportedly from another food company. The spoofed food company email used the name of the president and the company's actual physical address. The ingredient supplier ran a credit check on the company, extended a line of credit, and the first of two shipments – valued at more than $100,000 – was picked up from the supplier. The victim company refused to release the second load until payment was received, and realized the email address used by the criminals was a slight variation on the actual company's domain name. The victim company contacted the legitimate company, who indicated their identity had been used in similar scams with other companies.
- In February 2022, four different fraudulent companies placed large orders for whole milk powder and non-fat dry milk from a food manufacturer. The orders, valued at almost $600,000, were picked up, and the victim company was unaware something was wrong until they did not receive payment. In all four instances, real employee names and slight variations of the legitimate domain names were used.

RECOMMENDATIONS

The FBI, FDA, and USDA urge businesses to use a risk-informed analysis to prepare for, mitigate, and respond to cyber incidents and cyber-enabled crime. Mitigation recommendations to prevent, detect, and respond to BEC-enabled product theft schemes include:

- Independently verify contact information provided by new vendors or customers through reputable online sources like associations or business directories. Pay close attention to the verified company name and branding. For example, a scammer's email may reference "Acme Baking, Inc." instead of "The Acme Baking Company" and contain an off-color or pixelated logo which mimics the original.
- Carefully check hyperlinks and email addresses for slight variations that can make fraudulent addresses appear legitimate and resemble the names of actual business partners. Look for additional punctuation, changes in the top-level domain (i.e. ".com" vs ".gov"), added prefixes or suffixes, or misspelling of the domain.
- Regularly conduct web searches for your company name to identify results that return multiple websites that may be used in a scam, i.e. the actual website "abccompanyllc.com" may be spoofed by fake domains like "abccompany.biz", "abccompany11c.com", or "abcompanyllc.com".
- Look for grammar, spelling errors, and awkward wording in all correspondence, to include email or requests through company web portals.

- Ensure company policies provide for verification of any changes to existing invoices, bank deposit information, and contact information.
- Encourage employees to request clarification and report suspicious requests to their management prior to authorizing transactions.
- Confirm legitimacy of advance payment or credit requests when not previously required.
- Verify all payment changes, credit requests, and transactions in person or via a known telephone number rather than through a number or link provided in a suspicious email.
- Be skeptical of unexplained urgency regarding payment requests or orders, especially from new customers.
- Be wary of last-minute changes in wire instructions, account information, or shipping destinations as well as changes in established communication platforms or email account addresses.
- Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises. The FBI has BEC resources here.
- Implement a user training program with phishing exercises to raise and maintain awareness among users about risks of visiting malicious websites or opening malicious attachments. Reinforce the appropriate user response to phishing and spear-phishing emails.
- Immediately report any online fraud or BEC activity to the FBI Internet Crime Complaint Center at ic3.gov/Home/BEC.

Recommendations for information technology administrators to help prevent BEC-enabled product theft schemes and to prevent the company's email system from being used in a scam include:

- Enable anti-phishing and anti-spoofing security features that block malicious email.
- Enable multi-factor authentication for all email accounts.
- Prohibit automatic forwarding of email to external addresses.
- Frequently monitor the company email exchange server for changes in configuration and custom rules for specific accounts.
- Add an email banner to messages coming from outside your organization.
- Prohibit legacy email protocols, such as POP, IMAP, and SMTP1, that can be used to circumvent multi-factor authentication.
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Enable alerts for suspicious activity, such as foreign logins.
- Configure Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate email.
- Disable legacy account authentication.

RESOURCES

- IC3.gov – Contact the FBI Internet Crime Complaint Center to report incidents and find industry and consumer alerts.

- FBI.gov – Resources to educate yourself and avoid becoming a victim of crime and fraud.
- FDA OCI – Contact FDA Office of Criminal Investigations to report suspected criminal activity relating to FDA regulated products.
- CISA.gov – CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats. By requesting these services, organizations of any size can find ways to reduce their risk and mitigate attack vectors.