United States Coast Guard

Maritime Cyber Bulletin

Bulletin 002-16 **December 28, 2015**

SPOOFED BUSINESS E-MAIL USED TO TRY AND DEFRAUD MARITIME ORGANIZATION

Overview

This Bulletin is provided to raise awareness of recent attempted cyber fraud activity in the maritime domain and is designed to provide further information about the event and to:

- Provide an overview of tactics, techniques, and procedures (TTPs) employed by malicious cyber actors; and
- Provide prevention and mitigation information

Description

WHAT IS BUSINESS E-MAIL COMPROMISE?

Business E-mail Compromise (BEC) is a type of payment fraud that involves the compromise of legitimate business e-mail accounts for the purpose of conducting an unauthorized wore transfer. After a business e-mail account is compromised, actors use the compromised account or a spoofed account to send wire transfer instructions.

Most of BEC incidents involve the compromise of an e-mail account belonging to a business's Chief Executive Officer (CEO) or Chief Financial Officer (CFO), in order to send an e-mail to an

employee with the ability to conduct wire transfers. Additionally, other incidents involve the compromise of a vendor/supplier's e-mail account with the intention of modifying the bank account associated with that vendor/supplier. The latter scheme may also be labeled as vendor fraud and involves last minute change of the bank and account number for future payments.

In most cases, after the actors compromise the legitimate business e-mail accounts through social engineering or malware, they conduct reconnaissance to review the business's legitimate e-mail communications and travel schedules.

In some instances, actors have auto-forwarded e-mails received by the victim to an e-mail account under their control. This reconnaissance stage lasts until the actor feels comfortable enough to send wire transfer instructions using either the victim's e-mail or a spoofed e-mail account that is controlled by the actor. The difference in the spoofed e-mail account is very subtle and can be easily mistaken for the legitimate business e-mail address.

WHY IS IT SO EFFECTIVE?

Malicious actors utilize multiple methods to ensure their e-mail communications are successful. In some instances, actors have created rules using the compromised business e-mail account to send all communications associated with the actor's activity to the trash folder or to a hidden folder the victim is unaware of. A common theme in the CEO/CFO scheme is that the actors wait until the CEO/CFO is on official travel before sending wire transfer instructions, making it more likely that the individual would use e-mail for official business and therefore harder to verify the transaction as fraudulent. These requests will sometimes state that the wire transfer is related to urgent or confidential matters and must not be discussed with any other company personnel.

VERSIONS OF THE BEC SCAM

Based on reporting activity dating back to 2009, there are three primary versions of the BEC Scam:

> Version 1: A business, which often has a long standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or e-mail. If an e-mail is received, the malicious actor will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent.
>
> Version 2: The e-mail accounts of high-level business executives (CEO, CFO, etc) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing financial requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the company with instructions to urgently send funds to bank "X" for reason "Y".

Version 3: An employee of a business has his/her personal e-mail hacked. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from the employee's contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow-up on the status of their invoice payment.

Maritime Event Overview

In mid-December of this year, the U.S. Coast Guard was alerted to a BEC attempt against a U.S. port facility. During this event, a member of the company received an e-mail from an unknown individual posing as the company's CEO. The e-mail indicated that the company had an invoice that was due for payment and instructed the recipient to wire transfer $15,000.00 to a named individual. The e-mail provided specific payment details, including account number and routing information, for the transfer of funds. The recipient of the e-mail questioned the legitimacy of the transfer and contacted the company CEO to verify the request. The CEO indicated that they had not sent the e-mail nor authorized any transfer of funds. Further investigation revealed that the company CEO's e-mail address had been spoofed. An investigation into the incident pends by Law Enforcement.

Proliferation of BEC Activities

BEC is a global scam with subjects and victims in many countries. The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) has received BEC complaint data from victims in every U.S. state and from over 45 countries. From fiscal year (FY) 2013-2014, IC3 captured the following statistics:

- Total U.S. victims: 1198
- Total U.S. dollar loss: $179,755,367.08
- Total non-U.S. victims: 928
- Total non-U.S. dollar loss: $35,217,136.22
- Combined victims: 2126
- Combined dollar loss: $214,972,503.30

Due to the success of the BEC scam, the FBI assesses with high confidence that the number of victims and the total dollar loss will continue to increase.

Risk Mitigation

The key to reducing the risk from BEC is to understand the criminals' techniques and deploy effective payment risk mitigation processes. There are various methods to reduce the risk of falling victim to this scam and subsequently executing a fraudulent wire transfer. Some of these methods include:

- Use caution when posting to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details;
- Be suspicious of requests for secrecy or pressure to take action quickly;
- Avoid free web-based e-mail, establish a company web site domain and use it to establish company e-mail accounts in lieu of free, web-based accounts;
- Verifying a change in payment instructions to a vendor or supplier by calling to verbally confirm the request (the phone number should not come from the electronic communication, but should instead be taken from a known contact list for that vendor or supplier);
- Maintain a file, preferably in non-electronic form, of vendor contact information for those who are authorized to approve changes in payment instructions;
- Use out of band authentication to verify wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a phone Personal Identification Number (PIN) to verify the executive's identity, or sending the executive via text message a one-time code and phone number to call in order to confirm the wire transfer request;
- When the staff at a victim business is contacted by the bank to verify the wire transfer, the staff should delay the transaction until additional verifications can be performed; and
- Require dual-approval for any wire transfer request involving:
    - A dollar amount over a specific threshold; and/or
    - Trading partners who have not been previously added to a "white list" of approved trading partners to receive wire payments; and/or
    - Any new trading partners; and/or
    - New bank and/or account numbers for current trading partners; and/or
    - Wire transfers to countries outside of the normal trading patterns.

Reporting

The U.S. Coast Guard encourages victims of cyber-crime to report this activity to the National Response Center (NRC) at 1-800-424-8802. Additionally, victims are also encouraged to contact local law enforcement and their local FBI field office. A list of local FBI field offices can be found here.

Questions

For maritime cyber safety and security questions or questions related to this report, contact the U.S. Coast Guard Liaison Officer to the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) at:

Email: CGNCCICLNO@hq.dhs.gov

Phone: (703) 235-8850

Feedback

Your feedback is important to us. Please e-mail any comments and/or feedback on this product to CGNCCICLNO@hq.dhs.gov.