TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members and Partners

DATE: November 28, 2018

SUBJECT: BEC Scams Evolving to Target Direct Deposit Accounts via Email

Malicious actors are evolving Business Email Compromise (BEC) scams to target direct deposit accounts through emailed change requests sent to Human Resource or Finance departments. The Multi-State Information Sharing and Analysis Center (MS-ISAC) has received multiple reports of state, local, tribal, and territorial (SLTT) governments and private sector entities receiving a small number of spoofed emails. Of note, a significant majority of the employees who had their accounts spoofed were executive-level staff members.

This new variant utilizes a similar method of coercing targets to send money to the malicious actor as the previous BEC W-2 variant, which has resulted in significant data or financial losses for SLTT governments or employees. Further information about the BEC scam, including the Purchase Order, Wire Transfer/Financial Theft, and W-2 variants, is available in the MS-ISAC Security Primer.

INDICATORS

- Spoofed email address where the header information does not match the "From" line
  - Email address domains including "@lycos.com" and "@oitfri.com"
- Subject lines including "Direct Deposit Update!" or "Payroll Direct Deposit"
- Initial message bodies include text similar to:

  Hi <HR or Finance Employee's first name>*,*
  I changed my bank and will need to update my paycheck DD details, can the change be effective for the current pay date?
  Regards,
  <Employee's Full Name>

  -- OR --

  Hi <HR or Finance Employee's first name>,
  I have recently changed banks and like to have my benefit of direct deposit changed to my new account. I need your prompt assistance on this matter.
  Regards,
  <Employee's Full Name>
- Follow-up message exchanges between the malicious actor and HR or Finance employee may include authorization to "override" any protections in place, requests to send a voided check instead of filling out a form, or reasons why the spoofed employee needs assistance.
- Referenced bank information: Gobank (a division of Green Dot Bank), Routing #: 124303162
- Other indicators of BEC emails may include:
  - Poorly crafted emails with spelling and grammar mistakes, that include a note indicating the email was sent from a mobile device (e.g. iPhone, iPad, Android, etc.) in order to convince the recipient the mistakes can be ignored.
  - The wrong or an abbreviated signature line for the supposed sender.
  - The use of full names instead of nicknames and a language structure that may not match how the supposed sender normally communicates.
  - Indications that the only way to contact the sender is through email. In some cases, the emails appear to be timed to correspond with times the senior official is out of the office.
  - The transactions are for a new vendor or new contract.

- Originating IP addresses from outside the U.S., Tor nodes or Nigeria
- Internal warning banners that indicate the email is spam, spoofed, or from an external source.

RECOMMENDATIONS

- Immediately notify Human Resource and Finance departments employees of this new variant. Ensure they are aware how to report potentially malicious emails and have a policy for out-of-band verifications (e.g. verbal confirmations, etc.) of direct deposit or account changes or wire transfer requests.
- Flag emails from external sources with a warning banner.
- Craft a policy for identifying and reporting BEC and similar phishing email scams. Make sure to include the following:
  - When receiving unusual financial or sensitive data requests, users should verify the identity, authenticity, and authority of the email sender via non-email channels.
  - Users should ensure that the email is going to the correct person. The true recipient of an email can often be verified by hovering the mouse over the address in the email header.
  - Users should reply by forwarding, and not by hitting the "reply" button, which helps to prevent successful spoofing attacks.
  - Users should report suspicious emails to security staff. The MS-ISAC also appreciates receiving notifications of all BEC scam attempts.
- Develop a BEC Incident Response Plan.
- Collaborate with Human Resource and Finance departments to ensure their policies are supported by technological solutions.
- Report BEC scams to the MS-ISAC, local law enforcement, and the Internet Crime Complaint Center (IC3). Tax-related suspicious emails should be reported to the IRS. If there is a financial loss, notify the bank to stop payment and involve local law enforcement.

Please do not hesitate to leverage the MS-ISAC to assist you in investigating the incident or in your response and recovery efforts. We perform a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning. Requests for these services can be obtained by calling 1-866-787-4722 or sending an email to SOC@cisecurity.org.

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722