The Business Email Compromise Scheme

September 2015

Businesses globally continue to be impacted by a long-standing scheme that exploits executive email accounts and email-based invoicing procedures to execute fraudulent wire transfer payments to foreign banks.

U.S. law enforcement reports that Business Email Compromise (BEC) actors are evolving their tactics and becoming more sophisticated. Since late 2013, global law enforcement agencies have been tracking a scheme known as the BEC scam impacting a wide range of businesses and individuals. The scam includes multiple types of fraud including romance, lottery, employment and property rental schemes that all focus on facilitation of fraudulent wire transfers with funds being primarily sent to Asia.

Law enforcement and security researchers concur in openly available reports that the primary BEC scenario involves the compromise of a senior executive's corporate email account or the impersonation of a senior executive's corporate email address. An email appearing to be from the executive is sent to an individual who is responsible for processing wire transfers with a message to process the transaction immediately. This scenario relies upon executive-level authority to authorize such a transaction and conveys a sense of urgency so the employee will execute the fraudulent wire transfer without double checking the authenticity of the request.

A recently observed variation of the BEC scheme involves victims receiving emails or phone calls from fraudsters impersonating lawyers or representatives of law firms claiming to be working on confidential matters that require the victim to immediately process wire transfers. Victims have reported that this variation of the scheme typically occurs at the end of the business day or week.

There are other versions of the BEC scenario, one of which involves impersonation of a supplier with a long-standing relationship with a business. The business is asked via email, phone, or fax for payments to be wire transferred to a new account. If the business receives an email request for the transfer, it will likely be from a fraudulent email address, but closely resemble a familiar email address of the supplier. An example is the transposing of characters in an email address to obscure the sender that at first glance may be difficult to detect – johnasmith@gmail.com vs johncsmith@gmail.com.

Another version of the BEC scheme involves the compromise of an employee's personal email account and theft of information detailing how the business engages with suppliers, including who the business' point of contact is at the supplier. Using this information, the BEC actor will issue invoices from the compromised business employee's personal email account to the supplier and include new instructions for where to send fraudulent wire transfer payments.

As public knowledge about the BEC scheme has expanded, actors are using the following more sophisticated tactics to make their activity more difficult to detect:

- Actors have an intimate knowledge of how the victim organization processes internal wire transfer orders.
- When the actors compromise a victim's email account, they use rules to forward emails about their activity to hidden folders or files, making detection by the victim complex and unlikely.
- BEC actors have been observed waiting until executives are on vacation to act, relying on the fact that because these individuals are out of the office, employees will be less likely to question why the executive is emailing them instructions outside of the normal operating procedures and more likely to facilitate a fraudulent wire transfer.

As of August 2015, total global losses from the BEC scheme were $1.2 billion, with over 8,000 victims, according to data collected by U.S. law enforcement. Experts agree that the total victim and loss figures are low due to underreporting and that the total losses will continue to increase. This attack targets how your business processes wire transfers and exploits any potential vulnerabilities in those procedures. **Citi clients, along with customers of all financial institutions, are at risk of falling victim to this scheme.**

Information Security Best Practices to Counter BEC Schemes

- Avoid using publicly-available email accounts for business purposes – victims with open-source email accounts are the most targeted in BEC schemes as these accounts are easiest for the attackers to access and impersonate.
- Closely examine email addresses. Ensure that you check the entire email address and do not rely upon shortened addresses that some email providers substitute for the actual address-ie. JohnSmith instead of john.smith@gmail.com.
- The field following the @ sign in an email address is known as the domain name. When using a corporate email account, consider filtering email traffic to flag emails from domain names that are similar, but not identical, to either your domain name or your customer domain names. When possible, consider purchasing domain names that are similar, but not identical, to your company name to ensure these variations are not exploited for nefarious use-ie. legitimate domain: company-a.com possible attacker domain: company_a.com
- For individuals in the company who have been previously targeted, consider eliminating their ability to use the "Reply" function in email transaction requests. Instead, rely upon a secure list of addresses for contacts that are physically typed in during every email exchange.
- Determine if the number of individuals in your organization who have the authority to approve or conduct wire transfers can be reduced.
- Consider implementing procedures for verifying urgent or confidential wire transfer orders to eliminate this often used technique.
- Explore a second factor authentication method for receiving internal wire transfer requests. This can be as simple as a phone call or as sophisticated as a PIN system to authenticate the user placing the wire transfer request. This will enable the payment processor to authenticate if the transfer order comes from an authorized requester or if the legitimate email account is being used by an unauthorized user.
- Closely monitor high value transactions, new trading partners, new bank or account numbers, and transfers to any new countries. Once thresholds are established, implement maker/checker requirements to ensure anomalies are not overlooked in processing wire transfer orders.