Guardian Analytics Fraud Update
Revised March 2016

Guardian Analytics Fraud Intelligence

Business Email Compromise (BEC)

According to the latest figures from the FBI, cyber thieves have stolen $2 billion from 12,000 businesses[1] using a scam that starts when business executives' or employees' email accounts are compromised or spoofed. The fraudster is able to steal money with the help of an unwitting accomplice, an employee who is fooled into submitting a wire request. From the perspective of the company's financial institution, the transaction appears completely legitimate. Even confirmation calls or other out of band authentication will reach the employee who did indeed submit the request.

Description of the Scheme

Fraudsters Do Their Homework

There are at least three versions of this scheme. They all start with in-depth reconnaissance as the fraudster learns key details about their intended victim, how they're structured and who to target in order to make the emails as convincing as possible. They will try to compromise an employees email account to see what they can learn there, and will check publicly available information such as:

- Company web page
- Press releases
- Social media
- Out of office replies with travel schedules

They are looking for:

- General information about the company, where it does business, and with whom
- Names and titles of company officers
- Management organizational structure: who reports to who
- Information on new rounds of funding
- Information on new products and services, or patents
- Product or geographic expansion plans
- Travel plans

Once they know who to impersonate, who to target, and what message will be the most believable, they establish a means of emailing the fraudulent request. If they're able to compromise an executive's email account, they control email flow to avoid detection. They might set up Inbox rules, such as creating a rule to redirect or delete certain email within the attack, preventing the legitimate owner of the account from seeing these emails. Or they may edit the "Reply to" addresses so if someone replies to an email related to the scam, the reply goes to an email address set up by the fraudster.

If they haven't been able to compromise an exec's email account, they create a look-alike domain (a "spoofed" email domain), such as …@companyABDC.com instead of …@companyABCD.com, or …@company_name.com instead of …@company-name.com (underscore instead of a hyphen). Or they replace an "m" with an "r" and an "n".

Now that the fraudster knows what to say to whom, and how, here are some examples of specific attacks.

1. source: http://www.cnbc.com/2016/02/25/ceo-email-scam-costs-companies-2bn.html

Example 1: Email from a company executive

1. A fraudster compromises the email account of an executive, such as the CFO.
2. The fraudster sends a request for a wire transfer from the compromised account to an employee who is responsible for processing these requests and is subordinate to the executive, such as the Controller.
3. The Controller submits a wire payment request to the FI, as per instructions from her "boss."

A variation on this scam uses a spoofed email domain that is very similar to the actual company domain instead of having to compromise the email system.

Another version starts with mocking up a fake email from the CEO, for example, to the CFO. The criminal uses the CFO's compromised email account to forward the fake CEO email to the Controller asking that she issue the wire "at the CEO's request," adding urgency and legitimacy to the request.

A third, more recent variation of the scam has the fraudster sending an email, supposedly from the CEO, to employees in Human Resources or Accounting asking for W2 details on all employees, which the fraudster then uses to file fraudulent tax returns.

Example 2: Invoice from supplier or business partner via spoofed email address

1. A fraudster compromises the email of a business user employed by their target company, for example, someone in Accounts Payable.
2. The fraudster monitors email of the business user looking for vendor invoices.
3. The fraudster finds a legitimate invoice and modifies the beneficiary information, such as changing the routing number and account number to which payment is to be sent.
4. The fraudster spoofs the vendor's email to submit the modified invoice. It doesn't require compromising the vendor's email system, but instead sends the invoice from an email address that is so close to the domain of the vendor that most people would miss the change (see earlier examples).
5. The email explains that they (the vendor) has updated its payment processes, which explains the new account details.
6. Accounts payable, recognizing the vendor name and services provided, processes the invoice and submits a wire request for payment.

Example 3: Email from an attorney regarding a business acquisition

1. The finance department receives an email from a fraudster pretending to be the CEO regarding a secret company acquisition. The email emphasizes the sensitive nature of the deal, making the employee feel special by being included by the CEO in this confidential operation.
2. The email explains that an attorney working on the acquisition will follow up with the wire instructions.
3. The fraudster posing as the attorney follows up by email or phone with the wire payment details as the original email from the CEO stated he would.
4. The finance department submits the wire request for payment.

These schemes hinge on an email request that appears completely legitimate, either coming from an actual email account or one that is so similar that all but the closest scrutiny would miss the variation. The FBI alert warned, "The requests for wire transfers are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request." Gone are the days of the obvious warning signs of criminal activity, such as bad grammar and spelling, or unrealistic scenarios.

How to Detect Suspicious Wire Requests Resulting from the BEC Scam

To detect fraudulent payments submitted as a result of BEC, even if they are submitted by a legitimate employee, FIs need to look holistically at the wire details, how and when the request was submitted, and the relationship between the originator and beneficiary. The analysis needs to include the following, but seldom is an individual data point sufficient to detect fraud:

- Transfers amounts that are unusual (higher or lower) for a particular business account or vendor
- Payments to beneficiaries that are new, are outside of where the business typically operates, or international transfers, especially to APAC countries (China, Malaysia, Hong Kong), or Eastern Europe
- Changes in the requestor's (i.e. the employee's) established cadence of using online banking or a direct payment application for initiating wire payments
- Transfers to known vendors with new payment details: e.g. first time use of wire, or new beneficiary account information
- Changes in established vendor payment cadence (i.e. frequency per month) and/or timing (e.g. always early vs. late in the month)

Customer Outreach – A Delicate Conversation

The fact that this scheme is rooted in fooling an employee into submitting the payment request makes it particularly delicate for the FI when they uncover a suspicious transaction. Even if the FI detects the suspicious request before submitting it for payment, which is always preferred, it's important to manage the conversation carefully. The FI can expect the account holder to be embarrassed at being duped, to possibly deny that they requested the transaction, or to be quite upset.

Here are some suggestions for managing this conversation.

- Be prepared with all of the information about the suspicious transaction – how the request was submitted, the payment, the timing, history of other payments to the same beneficiary, etc.
- Start like a normal verification call, get the account holder talking to uncover details, gradually adding more questions, such as:
    - Can they confirm the account holder to which funds were sent – name and relationship?
    - Can they confirm the payment that was recently requested (specifically, the account number and the amount)?
    - What was the payment for?
    - Did this payment involve any activity that varied from their normal process or include any exceptions to established protocol?
    - Did the person who submitted the payment request (e.g. the controller) get a verbal confirmation from the person who sent the email (e.g. the CFO)?
- Help them see why you're suspicious; explain the scam and encourage them to re-confirm the request using an alternate contact method.
- Help the account holder understand you are there to help.
- Redirect the emotion. Refocus their attention on the pain that could be caused by a fraudulent wire costing them more than they probably can afford to lose, and the exec's reaction.
- Have an escalation process ready should the account holder become upset.

About Guardian Analytics – Guardian Analytics is the pioneer and leading provider of behavioral analytics solutions for preventing banking fraud. Hundreds of banks and credit unions have standardized on our solutions for detecting fraudulent wire and ACH payments, and preventing online and mobile banking fraud, including detecting fraud attacks like the one described above. As a result, they are improving competitiveness and growth, reducing fraud risk and losses, enhancing compliance, and increasing operational efficiency.