Guardian Analytics Fraud Update
October 2015

Guardian Analytics Fraud Intelligence

Business Email Compromise

According to the latest FBI alert[1], cyber thieves have stolen $750 million from 7,000 businesses using a scam that starts when business executives' or employees' email accounts are compromised or spoofed. Victims have increased by 270 percent since the initial FBI alert in January 2015. 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

There are at least three versions of this scheme. Here are descriptions of how two of them work. The third, featuring spoofed attorney emails, is out of the scope of this summary, but generally is similar to these two.

Payment request 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 a second employee within the company who is responsible for processing these requests and is subordinate to the executive. For example, 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.

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, for example, @companyABDC.com instead of @companyABCD.com.
4. Accounts payable, recognizing the vendor name and services provided, processes the invoice and submits a 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 compromised or spoofed email, even if they are submitted by a legitimate employee, FIs can look for the following:

- Transfers to known vendors with new beneficiary account information
- Transfers amounts that are unusual (higher or lower) for a particular vendor or business account
- International transfers, especially to APAC countries (China, Malaysia, Hong Kong), which the FBI alert notes is the typical destination for these wires
- Changes in established payment cadence (i.e. frequency per month) and/or timing (e.g. always early vs. late in the month) to known vendors
- 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
- First time use of wire to pay an established vendor or beneficiary

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, gradually adding more questions, such as:
  - Can they confirm the account to which funds were sent – name of account holder 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)?
- Get the account holder talking to uncover details; hold back on what you know to keep them talking. Once they realize the payment was fraudulent, they may not be as forthcoming with additional details.
- Help the account holder understand you are there to help.
- 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.

1. To read the August 2015 FBI alert, go to: http://www.ic3.gov/media/2015/150827-1.aspx