RANE
Risk Assistance
Network + Exchange

RANE Expert Advisory

Business Email Scams Lead to Increasing Wire Transfer Fraud

June 24, 2015

The following advisory was authored by Jim Mintz, founder and CEO of the Mintz Group, a leading international corporate investigations firm. Mintz co-founded The Investigative Group in 1984 and a decade later launched his eponymous firm. He is a founding member and director of the International Association of Independent Private Sector Inspectors General.

What is Happening

Over the past 18 months, a wide array of companies have fallen victim to a sophisticated email scam that the FBI, in two alerts issued this year, has dubbed the Business Email Compromise (BEC). This scam targets any kind of company that regularly makes wire payments, from small business to multinational enterprise, across industries. The criminal uses spear-phishing emails to gain entry to a corporation's internal systems, and then leverages trusted relationships between individuals who authorize wire transfers and those who send them out, costing firms real money.

- The Mintz Group is seeing approximately one new case every two weeks, with individual company losses ranging from $30,000 to millions of dollars.

- From October 2013 to December 2014, according to the FBI alerts, almost 1,200 organizations in the US were reported being victimized by the scam, with total losses estimated at $179 million; outside the US, another 928 entities lost a combined $35 million.

- According to the FBI, the BEC scam frequently starts when the executives whose accounts have been spoofed are traveling or out of the office. In many instances, the supposed recipient of the payment is a Hong Kong or Chinese bank account for a defunct Hong Kong company.

- The scam appears to be more prevalent in organizations that use open-source or free web-based email products, and in some cases the sender is suddenly using a personal email account to communicate.

What to Watch For

As with any spear-phishing attack, this scam, sometimes referred to as "CEO Fraud," begins by getting an unsuspecting employee to click on an email attachment that compromises the network. After that, it goes as follows:

- The person in charge of making wire transfers (often the CFO) receives an official-looking email with letterhead attachments from a high-ranking officer (often the CEO) asking that a payment be made immediately to a particular person at an overseas bank.

- In most cases, the email asks that the urgent transfer be "kept in confidence," and it sometimes identifies an employee in the accounting department to give an added (false) sense of authenticity.

- The amounts of money requested are tailored to be within the expected range of the payments that that particular enterprise would be making.

- The instructions at the receiving bank are to move the money as fast as possible, and all too often by the time the company realizes it has been duped the money is long gone.

- Often there are small hints in the fraudulent email that should be a red flag: the sending email address can end in *.co* rather than *.com*, or have a letter *L* replaced with the number *1*.

The FBI has identified two other variations of the BEC scam:

- An employee's hacked personal email account sends fraudulent invoices to a number of vendors requesting immediate payment to phony company bank accounts.

- A business receives a fraudulent invoice from a longstanding supplier asking to wire payment to an alternate account.

What to Consider

With email crime getting more sophisticated, ensuring that company policies and procedures are thoroughly articulated, understood, and practiced is essential. Additionally requiring a second authenticator for all requests for money transfers is a best practice to reduce the risk from the BEC scam. Finally, ensuring that every employee is sensitized to—and guarding against—the risk from spear-phishing is a critical line of defense against a wide range of cyber crimes.

- Requiring face-to-face or over the phone authorizations for all wire payment reduces the risk from email fraud.

- The FBI also suggests all parties use digital signatures on both sides of any transactions.

Related Reading

- *Federal Bureau of Investigation*, Business Email Compromise Alert, January 22, 2015
- *Krebs on Security*, Spoofing the Boss Turns Thieves a Tidy Profit, March 10, 2015