CARLTON FIELDS

Spoofing Whales: How Companies Can Protect Their CEOs and CFOs from the "Business Email Compromise"

July 20, 2015

Cyber scammers continually innovate new means to extract valuable information from unsuspecting victims. And a new form of cyber fraud is exploiting the close relationship between CEOs and CFOs. Identifying this threat — and the means to prevent it — is important for employees in IT, finance, and compliance. **Plenty of Phish in the Sea**

First, some definitions. “Phishing,” the use of online communications such as mass emails or recorded telephone calls to trick users into giving out sensitive information, has become routine. In phishing, the criminals often pose as a legitimate company to obtain financial or personal information. “Spear phishing” is a targeted phishing attack against specific individuals within specific companies, in which the fraudsters deploy personalized emails or other forms of online contact. Spear phishing’s high-achieving younger brother — “whaling” — uses the same techniques to aim tailored lures at upper management. Successive spear phishing often precedes a successful whaling attack, as the criminals climb the corporate ladder with the ultimate goal of parting the company from its money or committing corporate espionage. The “business email compromise” is a similar

scheme that targets businesses working with foreign suppliers. In this fraud, the criminal uses a spoofed or hacked email address of a business insider to prompt the business to transfer an urgent wire to the hacker's account. This article will explain a form of the business email compromise that borrows elements of whaling to target CEOs and CFOs. We will then suggest some methods to defeat it. In whaling, successful attackers first research the executive's social media sites, corporate webpages, and professional writing so that the email or phone call that lures the executive is tailored enough to avoid suspicion. The criminal's initial legwork also determines what level of access the executive has to company secrets or what might be the easiest way to part the executive from her money or credentials or the company's funds or intellectual property. The scammer may pose as the company's bank, the CEO's private banker, a BMW salesperson, or a family member. The goal of traditional whaling is often to obtain bank account or other personally identifiable information from the executive, for later use in identity theft. Although whaling is usually done in small numbers, perhaps the best known example is a large one. In 2008, scammers sent thousands of C-suite executives an email message that appeared to contain official subpoenas from a federal court in San Diego. The email text contained the executive's name, company, and phone number. The link embedded in the message promised access to the full subpoena, and, when clicked, prompted the recipient to first download a browser add-on. The downloaded file secretly contained a program that captured the executive's keystrokes, which it transmitted back to the hackers, capturing passwords and corporate information. In total, approximately 2,000 of the targeted executives fell victim. And these crimes persist. In May of last year, the U.S. Department of Justice announced the federal indictment of five Chinese military officials for what amounted to a major whaling operation waged against six U.S. companies. At one victim company, these officials allegedly posed as the company CEO in sending an email to approximately 20 employees, which contained a link to malware that allowed the officials "back door" access to the company's computers. **Re-Baiting the Hook**
The whaling version of the business compromise email, and a variant of the scheme that is currently in vogue, has a more immediate return —its sole goal is to part a company with cash. The scammer first either hacks into or spoofs the CEO's email address. A spoof is an email address that appears to be the same as the CEO's address, but is really sent from another, hidden email account. A spoof can also approximate the email address but, for example, insert an extra letter in the text preceding the "@," change the letter "l" to the digit "1," or add an alternate variation of the corporate standard, such as using "jeclabby@" (note the correct middle initial) rather than "jclabby@". After having achieved the ability to send an email that appears to be from the CEO, the scammer then sends an email from that address to another executive with the authority to wire a large amount of money on short notice, and this is often the CFO. This email will contain instructions to wire corporate money to a new account of a known corporate vendor or business partner, often at an offshore bank, and to do so as soon as possible. The CFO, wishing to be as responsive as possible to the CEO, will drop everything to execute the wire. By the time the company realizes the transaction was not authorized, sometimes by calling the actual vendor to confirm payment, the money is long gone from the recipient account or otherwise unrecoverable. This scheme succeeds because the spoofed email itself often contains a PDF file of an invoice that appears to be from a real company that does

business with the victim company and because the email text and header information otherwise contain the hallmarks of an actual business communication for the company. But the scheme also succeeds because the criminal has deployed techniques known collectively as "social engineering," a form of manipulation in which knowledge of human behavior is used to influence it. Through use of social engineering, the criminal gains money, information, or access not through fancy code or brute-force computer power, but through the more traditional tools of the midway grifter. In this case, the scammer marries an artificial sense of urgency ("this must be done immediately!") with the target employee's desire to please his boss. The scheme succeeds because the CFO's special relationship with the CEO fogs his vision of the fraud that is right in front of his face. **How to Stay Off the Dinner Plate**

Advice to lock your door at night does little to stop you from opening that door to a criminal who is dressed as a police officer. Similarly, firewalls and antivirus software have limited effect against a business compromise email targeted at senior executives in this fashion. The following tips will help you develop a program at your company to combat this type of fraud:

- Strengthen Controls Around Irregular Wires: Review and strengthen the controls around wire transfers, and, in particular, international wire transfers. This could include (i) requiring two forms of communication (both email and phone, both text and email, etc.) before a wire will issue; (ii) requiring approvals from two different persons apart from the requestor to initiate a wire; or (iii) authenticated contact with the recipient party at the supposed foreign vendor before an internally authorized wire will issue. In (i) above, another best practice is for the recipient of the CEO's request (in our examples, the CFO), to initiate the follow-up phone call to a known company or mobile number, rather than responding to "call me at xxx-xxx-xxxx with any questions," because the planted phone number could be a part of the spoof. Companies that face repeated attacks may also deploy more complex arrangements, including the use of rotating verbal passwords. Companies that have grown rapidly but that still rely on informal methods of communication surrounding vendor payment are particularly susceptible to this fraud.

- Improve Training for Finance Staff: Provide regular, periodic education to all executives and employees on computer fraud, including phishing and business email compromise, tailored to the particular employee's job description, so that they will understand the danger these attacks pose and spot potential fraud. This training should be tailored in summary fashion for the C-suite. For the line-level finance or treasury employees, including those who actually process wire transfers, training should include clear direction that suspicious wires may and should be questioned up the chain of corporate command, without retaliation, and that part of the employees' annual evaluation will include analysis of their contribution to fraud detection. Detection of this type of fraud can be included in the company's annual training on vendor payment fraud.

- Fund and then Audit Company Technology: Keep your anti-phishing software, operating system, and browsers up to date with the latest patches, and empower and fund your IT and data security staff commensurate with the risk that your company faces. Ensure that your regular penetration testing includes business email compromise, or other attempt to initiate a wire through direct emails to the finance staff.

The threat of whaling should be taken seriously by companies of all sizes, and particularly by companies that rely on fast-paced payments, that have vendors with multiple or changing receiving-bank information, and where executives work remotely from one another. In a matter of seconds criminals can compromise sensitive information, wire money internationally, and leave companies devastated. To minimize their susceptibility to such a breach, companies must arm themselves with a combination of awareness, training, and preparation of the IT defenses. **Removing the Hook**
If you believe your company has been the victim of such an attack, contact law enforcement, such as the Federal Bureau of Investigation, the U.S. Secret Service (through the Electronic Crimes Task Force in your city), or state or local law enforcement, to report it. If the attack is caught in progress or detected shortly after the wire transfer, get law enforcement involved *immediately*. Federal law enforcement's relationships with banks and the international money transfer system, in particular, may allow them to recover your funds or, at least, collect evidence for a successful prosecution. These attacks are embarrassing for senior executives and involve the loss of real money. As such, working through the aftermath to determine what happened, what if anything can be done to recover funds, and how to prevent a future attack, is a complex task. Consider involving experienced outside counsel to work on your behalf with law enforcement to sort through the evidence, monitor the efforts to track any disbursed funds, and otherwise protect the company's interests. When dealing with this kind of attack, the last thing a company needs is to be alone at sea. *The author thanks Colton Peterson, a rising third-year law student at Vanderbilt Law School, for his assistance with this article while a summer associate at the firm.*

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology