What's Worse Than Getting Phished? Getting Whaled

Five ways company execs can avoid the harpoon

By Devin Chwastyk / McNees Wallace & Nurick LLC

The internet and electronic communications have given rise to a plethora of innovative new criminal activities, some of which have entered the common parlance: phishing and its more targeted cousin, spear phishing, are chief among those schemes. Less well-known but still aptly named methods of online fraud include vishing (voice phishing) and SMiShing (text phishing).

Another still-emerging variety of scam is the "business email compromise," alternatively known as a BEC, CEO fraud or (most descriptively) executive whaling. These are like spear phishing attacks, only they target either high-level business executives, or, more commonly, they impersonate CEOs and others in the C-suite in order to instruct company employees to initiate wire transfers of corporate funds to the scam artists.

According to the FBI, between 2013 and 2016 the total loss from whaling attacks, from both U.S. and foreign businesses, was approximately $5 billion (U.S. businesses alone accounted for approximately $1.6 billion). Between 2015 and 2016, the FBI noted a 270 percent increase in reported victims of CEO scams, and many successful scams may go unreported.

Executive whaling is the new and improved "get rich quick" scheme for cybercriminals. These attacks are carefully executed by skilled cybercriminals to acquire money, or confidential and/or financial information from corporate data. Whaling attacks impersonate senior executives or other high-clearance level employees with access to highly sensitive information. These attacks take the form of fraudulent emails from senders posing as these trusted sources, requesting the release of confidential data such as employee tax returns or instructing the lower-level employees to send wire transfers.

Generally, the cybercriminal will gain as much information as possible on the CEO (or any other chief executive) by browsing public social media profiles or from information acquired from previous cyberattacks. The executive whaling attack email may be personally addressed, reference personal matters or previous lines of correspondence, and might demand a quick response to time-sensitive business matters. These attacks rely on employees not to question the boss and to comply quickly with those demands.

Some of these attacks have cost companies millions of dollars – and cost executives their jobs.

Executive whaling should not be confused with phishing or spear phishing. Although there are similarities between the three methods of cyberattacks, there are also key differences. Unlike executive whaling, phishing attack emails are simultaneously sent to a large number of employees within a company. These emails take a scattershot approach, hoping some of the many recipients might do whatever the email is asking of them, such as clicking on a link.

Spear phishing is more personalized than phishing but not as bespoke as executive whaling. The cybercriminal gathers information on the intended target, which is usually an individual or a small group of people within the company. Spear phishing attack emails generally include the target's name and job title, with an authentic logo of a business that the target has a relationship with (such as a logo of their bank) to make the email seem more trustworthy to the target.

Overall, the objective of these three methods is to maliciously deceive recipients, either into disclosing sensitive information, clicking a link or downloading an attachment to introduce malware into their computer system or voluntarily comply with the sender's request by impersonating a trusted figure.

When a company has been victimized by an executive whaling attack, it is common that the chief executive(s) of the company take the downfall. In January 2015, an internet money transfer service in San Francisco lost $30.8 million, resulting in the CFO resigning. A financial services software firm in Windsor, Connecticut, lost $5.9 million in September 2016, resulting in the CEO being ousted and the company facing a $10 million lawsuit. Once funds have been lost through executive whaling attacks, it is rare that the business will be able to recover even a portion of the money. There are no zero-fraud guarantees to remedy fraudulent wire transfers, as there are with some credit cards. Indeed, most state laws relieve the bank of any liability so long as the sender followed agreed-upon procedures for authorization of the transfer. This makes CEO fraud especially damaging, as lower-level employees will follow those exact procedures at the behest of the boss.

However, there have been a few instances where companies have been fortunate enough to recover some funds. In January 2016, an aerospace company in Austria lost $50 million, but managed to recover $10.9 million of it. Nevertheless, the CEO and CFO were still fired. In April 2016, a toy manufacturing company in El Segundo, California, proved even luckier: It immediately caught the attack and was able to fully recover all $3 million.

The potential of an executive whaling attack is very real, and every company should take proper precautions to avoid such attacks. They include these five:

1. All executives should keep their social media profiles private, given that cybercriminals gain a lot of their intel from social media.
2. If the executive chooses to have a public social media profile, there should be little to no personal information on it (such as birthdays, hobbies, memberships and friends).
3. Executives, accounting staff, IT staff and HR staff should be trained to spot characteristics of a whaling attack email, and a two-factor verification should be required before a wire transfer can be approved (for example, an authorization by telephone from a trusted number confirming the transfer).
4. Mock whaling attacks should be conducted regularly to test employees.
5. A rigid security policy regarding the release of employee records and wire transfers of large sums of cash should be established.

Devin Chwastyk *is the chair of the privacy and data security group at McNees Wallace & Nurick LLC. He can be reached at dchwastyk@mcneeslaw.com. Sarah-Julie Tchokouani, a 2017 McNees summer associate, contributed to this article.*