security

Whaling and CEO Fraud: a case for company culture

Paweł Wałuszko 26.08.2020

Whaling – phishing attack aimed at top managers and C-level executives

CEO Fraud – a social engineering attack in which the attacker impersonates a C-level executive

When someone thinks of a phishing attack, chances are they're envisioning a simple, poorly-written message, littered with spelling and grammatical errors. Oftentimes this message is embellished with pixelated, out of proportions graphics, which only adds to its lack of credibility. Of course, nobody takes these messages seriously, and rightly so.

A step up from a *phishing* attack is a *spear phishing* attack. In this type of an attack, the scammer invests a little bit more of their time in order to create a more convincing message. These types of emails are more personalized. They may appear to come from a business partner or mention important events in the company.

Targeting lower and middle-tier employees can bring hackers decent results. According to Verizon's *2019 Data Breach Investigations Report* and research conducted in 2019 for Canon, about 30 to 34% all data breaches are a result of the so-called "insiders". These insiders are, among others, employees who unknowingly cooperate with hackers by providing them sensitive information.

Decent results, however, are not great results. Even when the attackers manage to obtain an employee password, their scope of damage can be quite limited. Most companies utilize different passwords for every service and limit employee data access by department, role and duties. Moreover, most IT departments tend to utilize the Principle of Least Privilege: granting the user only the minimum necessary rights in order to complete a task. This is all not to say that employee credential leaks should be treated lightly. However, such a leak is definitely not the data jackpot hackers could be hoping for.

CEO Fraud

What does Snapchat and Seagate have in common? They're big corporations. Both operate in the technology industry, although Snapchat produces software and Seagate produces hardware. What they have in common since 2016, however, is the fact that they have been victims of the largest data leaks obtained through the *CEO Fraud* method.

CEO Fraud is a social engineering attack, mostly carried out through email. In comparison to an average phishing attack, this type of attack is rather sophisticated: messages refer to real names and company events, utilize the victim's real-world mannerisms and ways of conveying information. On top of *mail spoofing* – which is making it look like the email came from a legitimate address – CEO Fraud messages even appear legitimate, as they tend to make use of corporate signatures and stationary in order to boost their credibility.

How do criminals get this data? Actually, it's rather simple. All it takes is a little bit of information digging and correlating data gathered from different sources. For example, finding out company stationary is as simple as writing an email to a C-level executive. Any reply, even "don't write to me again" is good enough, as long as the hacker gets to see what signature and stationary the executive uses. Reading press releases, company blogs and case studies brings in a wealth of data on company's

current and past clients. Social media, on the other hand, often exposes inner-company events, which otherwise would not be made public. In some social media posts there are links to videos, where you can see how the CEO articulates his/her points as well.

Armed with this knowledge, hackers get to work. Mail spoofing is a relatively simple procedure – all it takes, is one line of code. Even if the IT department of the targeted company took care of that security loophole (we recommend setting up DKIM, SPF and DMARC), there are dozens of ways of getting that email inside. One of the popular ways has been utilizing the "send on behalf of" feature in Microsoft Outlook, where a hacker could use employees' compromised account to send an email on behalf of the CEO.

Does it work? Of course it works (!) and perhaps the best case-and-point examples are Seagate and Snapchat. In 2016, an employee made a grave mistake of sending financial information (including tax information) of 10,000 Seagate employees to who he thought was – the CEO. The e-mail asking for employee W-2s was so believable, that it passed the careful eye of personnel and technological solutions, which could have prevented the e-mail from reaching its targeted user. In the same year, Snapchat had a similar misfortune. An employee responded to a data request which appeared to have come from the boss, but actually came from hackers. All in all, companies had to publicly admit the security mishap and compensate their employees.

In the meantime, some time has passed since 2016 and things took a turn... for the worse. According to the FBI, between 2016 and 2019 BEC (*Business Email Compromise, CEO Fraud*) was responsible for generating $26 billion in damages. Meanwhile, between 2018 and 2019, the amount of BEC/CEO Fraud attacks went up by 100% (Source: https://www.ic3.gov/media/2019/190910.aspx).

Whaling

The main difference between *CEO Fraud* and *whaling* is the fact, that in the latter, the CEOs are the target. In other words, hackers are going for the big fish.

These types of phishing attacks are a bit harder to carry out. However, when successful, they bring in the jackpot. Unlike mid-tier managers, C-level executives have virtually unlimited access to company data; they're not bound by information compartmentalization and can request any employee to carry out a data-sensitive task without doubting their reason.

One may be inclined to think that due to the sheer power of authority within a company, C-level executives enjoy the best level of protection from hacking attempts. However, this is not always the case. Firstly, there are no technological solutions which can guarantee absolute data security. Secondly, human error runs afloat. A recent example of a CEO's minor mistake and technological failure resulting in massive data breach is the case of Jeff Bezos' phone hack, which we outlined here. In short, hackers exploited a security hole in Apple's iOS by sending a malware-infected message through the popular communicator, WhatsApp. The CEO clicked on the link and all things went south from there (more on that here).

Serious business

It's worth noting that hacking C-level executives is a lucrative business. Even if compromising an entire device – as was the case with Amazon's CEO – is not possible, stealing even one password can bring in serious money. Intellectual property can be stolen or passed on to competitors, private information can be used to blackmail or discredit, and a single ransomware attack can generate a sizable income, especially when deployed on a privileged, "access granted everywhere" account.

Not surprisingly, even a CEO's Twitter password has it's worth. In July 2020, Twitter experienced one of the largest data breaches thus far. Accounts belonging to people such as Elon Musk, Barack Obama and Joe Biden were compromised. Hackers posted a COVID-related message, urging followers to take advantage of a one-time charity giveaway: send your money to me, I'll send it double (more on that in this article). The sheer authority of the owners of these Twitter accounts was clearly enough for some followers to send $115,000 in just a few minutes.

Establishing procedures and sticking to them

In cybersecurity, the best rule is having rules. The second best rule is actually following them.

When it came to the CEO Fraud attacks of 2016, employees should not have compiled and sent data, to which the CEO most likely already had the access to (such as through internal accounting software). Moreover, when requesting highly sensitive data, there should have been a protocol of double-authentication, even by a simple phone call.

Whaling attacks also exist because of human error, and no CEO is safe. There are no hack-proof devices and, as the case of Jeff Bezos reminds us, all it takes is a momentary lack of judgment. Therefore, if a message, pop-up, a file, macros or any communication appears out of the ordinary, it's best to forward it to the IT department for a closer inspection. Neglecting this extra step can open up a Pandora's box to new experiences.

Red teaming, vulnerability assessments and solidifying knowledge

Cyber-resilience of VIP personnel does end with establishing basic procedures and patching up key systems. Procedures – just as security solutions – work only when they're properly executed.

According to Canon, only 17% of cybersecurity incidents are caused by external cyberattacks. Majority of the incidents – 55-59%, are a result of the 'human factor', which can be as simple as everyday on-the-job mistakes, device misconfigurations, lack of adherence or misunderstanding official procedures. In order to address these human factor problems, a business must take an all-encompassing, company culture approach to cyber-resilience, rather than counting on rules and technology to solve the issue. Here a few ideas to consider:

- **Red Teaming** is an adversarial-based attack simulation aimed at employees, hardware and software along with breaching the companys' physical security. The exercise is performed in order to find weak spots in a company's cyber-resilience stance from a hackers' point of view (more on that here).
- **Vulnerability Assessments** are a review of the company's IT security posture from a strictly technical point of view. The outcome of such assessment is a clear outlook on current strong and weak-points, as well as recommendations and guidance on how to additionally secure the systems (more on that here).
- **Trainings** make sure that the employees are aware of their role in safeguarding company data, understand procedures and technological reasons for everyday modus operandi. Trainings should also provide best practice guidelines and technological know-how in case of social engineering attacks.

Takeaway

CEO Fraud and *whaling* are types of social engineering attacks, aimed at impersonating or deceiving an executive to divulge sensitive data. However, it's not necessarily the technology that fails us, but rather, lack of foresight regarding the 'human factor' in cybersecurity. In order to limit the probability of a human error and maximize cyber-resilience efforts, it's best to develop and promote a security-conscious company culture.

26.08.2020

Paweł Wałuszko

Business Development Manager and Cybersecurity Expert at TestArmy CyberForces. Experienced IT manager with background form the Silicon Valley; open-source enthusiast.

Cyberbezpieczeństwo e-commerce. Co grozi sklepom internetowym?

Insiderzy. Kim są i jak zagrażają Twojej firmie?