Definition of a Whaling Attack

A whaling attack is a targeted attempt to steal sensitive information from a company such as financial information or personal details about employees, typically for malicious reasons. A whaling attack specifically targets senior management that hold power in companies, such as the CEO, CFO, or other executives who have complete access to sensitive data. Called "whaling" because of the size of the targets relative to those of typical phishing attacks, "whales" are carefully chosen because of their authority and access within the company.

The goal of a whaling attack is to trick an executive into revealing personal or corporate data, often through email and website spoofing.

Tips for Defending Against Whaling Attacks

You may not be able to prevent yourself or your company's executives from being targeted in a whaling attack, but there are steps companies should take to reduce the likelihood that these attacks will be successful. Here are a few tips for protecting against whaling attacks:

- **Educate senior management:** Senior management, key staff, and financial teams should be educated about the effects of whaling attacks and how to spot them. Train these employees on the common characteristics of phishing attacks like spoofed sender names, unsolicited requests/attachments, or spoofed hyperlinks and conduct mock whaling attacks to test employees regularly.
- **Have private profiles:** Executives should have as little personal information on their public profile as possible; birthdays, hobbies, friends, and addresses can all be used in an attack. The best way to prevent unknown individuals from viewing personal details is to use privacy restrictions.
- **Mark external emails:** Many whaling emails are intended to look like they come from someone high up within the organization. A good way to spot potential whaling attacks is to flag emails that are sent from outside of the corporate network.
- **Establish a verification process:** If an employee receives an email requesting funds or information that is not usually transferred via email, the safest option is to verify the request with the stated sender via another channel before transferring any sensitive data. Have documented internal processes and train employees on how these requests should be handled.

- **Implement data protection:** Solutions like data loss prevention provide a critical last line of defense against whaling and other forms of social engineering attacks, preventing the exfiltration of sensitive data even in the event that an employee is tricked into attempting to send it to an attacker.

Why are Whaling Attacks Successful?

Whaling attacks use fraudulent emails that appear to be from trusted sources to try to trick victims into divulging sensitive data over email or visiting a spoofed website that mimics that of a legitimate business and asks for sensitive information such as payment or account details. Whaling emails and websites are highly personalized towards their targets and often include targets' names, job titles, and basic details to make the communications look as legitimate as possible.

Attackers also use spoofed email addresses and actual corporate logos, phone numbers, and other details to make attacks seem like they are coming from trusted entities such as business partners, banks, or government agencies.

Whaling attacks are more difficult to detect than typical phishing attacks because they are so highly personalized and are sent only to select targets within a company. Whaling attacks can rely solely on social engineering to fool their targets, though some cases will use hyperlinks or attachments to infect victims with malware or solicit sensitive information.

Because of the high returns that cybercriminals can gain from whaling attacks, attackers spend more time and effort constructing the attack to seem as legitimate as possible. Attackers often gather the details that they need to personalize their attacks from social media such as Facebook, Twitter, and LinkedIn, profiling targets' company information, job details, and names of coworkers or business partners.

Whaling is becoming more successful, and as a result there has been an increase in its popularity.

Examples of Whaling Attacks

Because whaling attacks are so difficult to identify, many companies have fallen victim to these attacks in recent years. In early 2016, the social media app Snapchat fell victim to a whaling attack when a high-ranking employee was emailed by a cybercriminal impersonating the CEO and was fooled into revealing employee payroll information. Snapchat reported the incident to the FBI and offered the employees who were affected by the leak two years of free identity-theft insurance.

Another similar incident happened in March 2016, when an executive at Seagate unknowingly answered a whaling email that requested the W-2 forms for all current and former employees. The incident resulted in a breach of income tax data for nearly 10,000 current and former Seagate employees, leaving those employees susceptible to income

tax refund fraud and other identity theft schemes. Seagate notified the IRS of the data breach.

Whaling vs. Phishing and Spear-phishing

Whaling attacks can easily be confused with phishing attacks because of their similar natures.

Phishing attacks and whaling attacks are both online attacks on users that aim to acquire sensitive information. Phishing is a broader term for any attempt to fool victims into sharing confidential information such as usernames, passwords, and financial details for malicious purposes. During typical phishing attacks, cybercriminals will send fraudulent emails to large amounts of victims in hopes that a small percentage will be successful.

Conversely, whaling is a special type of phishing that targets a high-ranking individual such as an executive rather than a large group of victims. Whaling emails are sent to a single person or small group of targets instead of the mass distribution techniques used in typical phishing attacks, and whaling attacks further differ from phishing attacks in that they are far more personalized and more closely imitate legitimate emails.

Whaling is a form of spear-phishing, a form of phishing which targets a particular individual to gain sensitive personal or business information. The key difference between whaling and spear-phishing is that whaling attacks target specific, high ranking victims within a company, whereas spear-phishing attacks can be used to target any individual.

Both spear-phishing and whaling take much more time and effort to execute than large scale phishing attacks because the attackers need to gather personal details on their targets and make emails seem as legitimate as possible.