Whaling Attack

Mukul Kumar
Gaurav Kabra
Priyanshu Singh

April 22, 2019

What is Phishing ?

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victims machine.

How does Phishing work ?

Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the targets computer.

Types of Phishing Attacks

- **Spear Phishing:** Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a companys defenses and carry out a targeted attack.

- **Whaling:** When attackers go after a big fish like a CEO, its called whaling. These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials. Whaling is of particular concern because high-level executives are able to access a great deal of company information.

- **Pharming:** Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site. Attackers can infect either the users computer or the websites DNS server and redirect the user to a fake site even if the correct URL is typed in.

Introduction to Whaling

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.

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 Attack

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.

Attacks involved in Whaling

- **ARP Poisoning Attack:** Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

- **Man in Middle Attack:** A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own.
  In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication.

- **Packet Sniffer:** A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.Attacker store the incoming and outgoing data into the packet using network sniffer tool.Apart from network sniffer,lots of packet sniffer and packet analysis tools is available which is used to check the sniffed packed.

Tips For Defending Against Whaling Attack

- **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.