Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Volume 3 Issue 3 **Dt: 01.05.2026**

Whaling

A Whaling Attack, also known as Whaling Phishing, is a strategic phishing attack, targeted towards high profile executives, that is disguised as a permitted email. An attacker can prod the target for information that helps them access sensitive areas of the network, passwords, or other user information.

A whaling attack can happen quickly, but it is often executed over the course of weeks or months. When a senior user interacts with the attacker, the attacker's goal is to establish the target's genuine trust. Taking the attack to the next stage too quickly may result in the target getting suspicious. However, if the attacker slowly proves that they are who they claim to be, the target may have no problem handing over sensitive information.

How Whaling Attacks/Whaling Phishing Works

A whaling attack may begin with a communication through a method commonly used by both the person being impersonated and the target.

This may be email or office texting that uses the internet. When the attack begins, there may be no reason for the target to question the identity of the attacker, as the latter may have the same username as the target's associate. In some cases, the email address may be faked, but it appears real enough to be believable.

The attacker may first seek to infiltrate the email account of the person they are using to get to the whale. Once inside, they can initiate an email that helps build trust. This may need to include a detail about the whale's life that the associate being impersonated would know. This kind of information can be easily gleaned off social media.

For example, the attacker may notice that the victim recently got a new puppy and posted about it on social media. They could then scroll down to the previous year's Christmas party and see that there was a huge cake. They could use the combination of both pieces of information to compose a seemingly innocent and appropriately knowledgeable email: "Hey, that cute little puppy's been getting big, huh? Had he been there last Christmas, I bet he could have devoured that whole cake!!! Lol!!!" Because of the detailed nature of the email, the whale may not suspect the attacker is falsifying their identity.

Once trust has been gained, the attacker could try to get secret information from the whale. For instance, they could say, "Ay, I'm on the road, and I don't have my log-in for the VPN. Could you shoot it to me real quick?" They could also try to gain access to proprietary information by making a request like, "Listen, I put those blueprints on my laptop, but I am using my phone right now. You mind sending those over real quick? I gotta meet this deadline." Because the whale believes the messages are legitimate, they may send over the information.

What Is The Goal Of Whaling Attacks/Whaling Phishing?

A cyber criminal unleashes a whale phishing attack for any of the following reasons:
Money: Attackers use spear phishing to deceive victims into wire-transferring money to them.
Control: A hacker who has obtained credentials to a company's network may move laterally to other parts of the network—or manipulate someone into giving them administrator access.
Attacks on supply chains: These occur when hackers gain access to weak points in a company's supply chain.
Corporate espionage: If a hacking attempt is successful, a hacker may steal trade secrets or other intellectual property to help rival companies, including those in other countries.
Malware distribution: Keyloggers, ransomware, and rootkits are just a few examples of the types of malware that a cyber criminal might trick whaling attack victims into installing.
Personal vendetta: The reputation of a whaling attack victim could be severely damaged, motivating someone with a vendetta to orchestrate an attack.

How To Block Whaling Attacks Or Whaling Phishing

You need a multi-layered strategy to thwart a whaling attack:

1. Some whaling attack emails may be stopped at the email gateway using robust anti-spam and anti-malware applications.
2. If an email is sent from a given domain, Domain Name System (DNS) authentication services using the DMARC, DKIM, and SPF protocols can determine whether it is valid or fake.
3. Email scanning and filtering software can be used to scan emails in real time to identify suspicious links or attachments, as well as block users from viewing them.
4. Anti-impersonation software recognizes the social engineering tactics frequently used in whaling emails and therefore can prevent a whaling attack.
5. Conduct security awareness training to help users recognize whaling attacks and enforce predesigned rules, such as confirming a money wire before taking any action.

How To Protect Yourself From Whaling Phishing Attacks

The first step in protecting you and your organization from whaling attacks is to educate all potential targets, as well as those that may be used to try to gain access to them. Because this could include a large proportion of your company, it may be best to include a "how to avoid whaling attacks" discussion during a training on other types of phishing threats.
Avoiding whaling attacks begins with a shift in mindset. When you read an email from someone, you should ask yourself if you were expecting to receive a communication from that specific person. Also think about whether there is anything strange about the email, including not just what is being said but how it is being expressed, the use of punctuation, emojis, or anything else that seems out of the ordinary.
In some cases, it is very obvious that you are being targeted. For example, if the email address is plausible but not the typical email the person uses, that is a telltale sign. For example, if the person usually uses the email account JSmith@yourorganization.com, but you get an email from JohnSmith@yourorganization.com, you should beware. If there is no reason why John would have to get another email address, this one could be fake. Further, if the email has a name that makes sense but comes from outside the organization, that could also be a sign of danger.
In addition, executives need to be careful about what they post on social media. Details about their lives can be used to execute whaling attacks. If a high-level member of the organization gets an email that mentions things they posted on social media, it may be an attempt to gain their trust in preparation for an inquiry for information.