What is whaling in cybersecurity?

As the name suggests, “whaling” in a cybersecurity context is a type of hyper-specific phishing attack designed to maximize impact by focusing in on senior/high-level executives and leadership teams within an organization. Typically, whaling attacks will take the form of emails targeted at c-suite executives or their equivalents. They are characterized by their studied understanding of the organization they are preying on, acquiring such an intimate knowledge base of its operations, decision-makers, and culture, that they are able to shape their tone and language in a way that manipulates unwitting employees to take actions on their behalf.

They often contain personal information pertaining to their recipient to gain their trust. This approach allows them to leapfrog the need for technical knowledge by using these individuals, their knowledge, and their network within the organization as tools in service of their greater objective. Much like a fly that comes to rest on a spider web, targets often don’t realize what’s happened until it’s too late. As such, scammers have access to huge potential rewards for relatively little prior investment or effort.

What is a whaling attack?

Whaling attacks rely on manipulating an individual into performing secondary actions against the best interest of their organization, some of the most common examples include:

- Opening a link to a site that delivers malware
- Transferring funds or requesting a transfer of funds to the attacker’s bank account
- Breaching data protection by providing additional details about the business, individual, or individuals to facilitate further attacks

How do whaling attacks work?

Whaling attacks hinge on the ability to either directly manipulate a high-value individual or masquerade as a high-ranking individual within an organization to influence the behavior of their peers or subordinates. In the case of subordinates, whaling often leverages the reluctance of junior staff to refuse or even challenge a request from their superior.

Peer-to-peer manipulation tends to rely on the compartmentalization of organizational duties i.e. the left hand not knowing what the right is or should be doing. Relationships that exist outside the business, such as those with third party vendors, are a common disguise for these kinds of attacks.

Whaling vs phishing attacks

Whaling emails share common goals and tactics with regular phishing and spear-phishing emails. They all employ techniques like email spoofing, fraudulent websites, and public data capture to compromise an organization's security. These methods facilitate the acquisition of sensitive and valuable information or money from the organization. The difference lies in their target: phishing scams take a blanket approach, hoping to pry information from anyone who will part with it. Whaling, in contrast, uses an ultra-specific approach, focusing solely on high-ranking individuals.

Examples of whaling attacks

Seagate

In 2016, an executive of **Seagate's HR department** was targeted in a whaling attack that resulted in the exposure of over 10,000 employees' income tax data, leaving them vulnerable to income tax fraud and identity theft.

Mattel

Mattel suffered a theft of $3 million in 2015 after the attackers posed as the company's CEO and targeted a C-level executive to action a transfer of funds to a new account.

Ubiquiti Networks

The same year, attackers targeted the CEO of **Ubiquiti Networks** by impersonating a third-party vendor requesting a transfer of funds, resulting in a loss of $46.7 million.

FACC

In perhaps the most famous incident of whaling to date, Austrian aerospace firm FACC lost approximately **$54 million** after attackers imitated its CEO in order to alter company banking details and move funds out of the company.

Is your company vulnerable to a whaling attack?

Although these examples all feature large companies and are high profile in nature, any organization can be vulnerable to whaling attacks. While larger organizations may represent a bigger potential prize to attackers, as well as have a greater capacity to be damaged by them, they also have considerable resources to fund cybersecurity and training programs in their defense. Small and medium-sized companies may simply not have the time, financial resources, or people to mount an effective defense against threats as insidious as whaling.

Recognizing a whaling attack

Since attackers will utilize the information gathered during their reconnaissance of personnel, they can often be more difficult to identify. Here are some common traits of a whaling attack:

- Spoofed emails: Whaling attacks will often forge either the personal or domain sections of an email address to look almost identical to a genuine contact which projects credibility and allows them to exploit the recipient's trust.

Additionally, many attacks mimic the templates, language, and tone of an organization when emailing an employee. It's also common for these emails to be sent with an air of urgency, creating psychological pressure on the recipient to acquiesce to the senders' requests quickly and making them more likely to overlook discrepancies or refrain from asking questions.

- Suspicious links: Links, attachments, and landing pages are used to sneak malware into vulnerable devices or networks and can be further concealed by embedding them into the main body of text of an email or other internal communication.
- High-value targets: Whaling attacks will almost always target high-value individuals in an organization with the goal of using their influence to either directly facilitate an attack or to direct others to do so on their behalf.
    -

How to protect your company from a whaling attack

While whaling attacks are as sophisticated as they are insidious, there are ways of shoring up and strengthening your organization's defenses to improve the chances of early detection and harm reduction in the case of a breach.

Start with the most vulnerable targets

C-Suite executives, management teams, specialist staff, and individuals with access to financial information are all likely targets for whaling attacks. As such, you should invest in training so that these vulnerable targets remain vigilant to the signs of a possible whaling attack, and to take swift action when one is identified.

Train your high-value employees to check the domain name of questionable senders, confirm high-risk requests via a separate channel, and avoid opening unsolicited attachments.

Create Operational Security (OPSEC) Awareness

The purpose of OPSEC is to identify otherwise innocuous activity that could leave individuals or your organization at risk if exploited. A common example would be your executives displaying personal information such as birthdays or hobbies on a public social media profile that an attacker could utilize while impersonating them. Company waste bins are also a common hunting ground for determined attackers and can provide useful personal or operational data to be leveraged later. The key is to identify these weaknesses and develop preventative policies or active countermeasures against them.

Install robust email security policies

Since email spoofing is often central to whaling attacks, ensuring you have the correct DKIM, DMARC, DNSSEC, and SPF settings in place can be extremely valuable as well as providing a means to flag suspicious external communications.

Create two step verification procedures

In addition to cybersecurity training, it’s also wise to create a culture of verification with universally understood protocols. No single employee, including C-Suite executives, should be able to request funds or sensitive data not normally suitable for email without prior verification in a separate channel. An internal messaging platform is ideal here since every employee is likely to have access as a matter of course. Document this protocol and ensure that it is well understood across your organization. Great opportunities to do this are employee onboarding sessions and quarterly organization-wide cybersecurity training “top-ups”.

Invest in anti-phishing technology

Anti-phishing technology works to highlight and block phishing communications. It can provide automatic scans of links and attachments in emails and prevent users from accessing them if they appear to be suspicious. Acquiring such technology can provide another layer of contingency to help protect both your employees and your organization as a whole.

How can Elev8 protect you from whaling attacks?

Elev8 provides bespoke, interactive digital skilling programs that can bring your teams and executives up to speed on the latest in cybersecurity insights, protocol, and best practices. They will learn why it is so important to remain vigilant against whaling attacks, how to recognize and respond to warning signs, and how to develop effective systems for prevention and harm reduction.

If you’re looking for an end-to-end skilling solution to empower your organization to prevent whaling attacks and other types of phishing, **contact elev8** for a consultation.