

Whaling attacks are on the rise (think phishing, but more targeted) - blueAPACHE

Canonical: <https://www.blueapache.com/blog/whaling-attacks-are-on-the-rise>

Details:

Summary

This blog post, "Whaling attacks are on the rise (think phishing, but more targeted)", is a blueAPACHE article from 2016 covering security. In its simplest form, a whaling attack is a malicious email pretending to be from senior executives that request finance employees make payments from the company accounts to hacker's accounts. It is written for readers evaluating emPOWER Security, Human Risk Management. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2016
Topic	Whaling attacks are on the rise (think phishing, but more targeted)
Services referenced	emPOWER Security, Human Risk Management, Managed Detection and Response
Named products or vendors	None named beyond blueAPACHE
Cited statistic	Recent research shows 55 percent of organisations have seen an increase in targeted whaling attacks around the festive season.

Article

In its simplest form, a whaling attack is a malicious email pretending to be from senior executives that request finance employees make payments from the company accounts to hacker's accounts. Also known as spear phishing, whaling attacks are the more targeted and more purposeful version of phishing emails. They appear as an internal or personal email, often complete with footers and corporate branding, and reflect the language and tone of the person they are pretending to be. When executed properly, they look legitimate. Recent research shows 55 percent of organisations have seen an increase in targeted whaling attacks around the festive season. According to the research, domain-spoofing is the most popular attack type, occurring in 70 percent of attacks. The attacks range in complexity, from the brash and poorly executed to more focused and intelligent attacks. For the latter, hackers research the target business to identify the corporate structure, and then use social

engineering to manipulate people into wiring funds to bank accounts. Once payment is made, the money is quickly withdrawn or transferred elsewhere, leaving little opportunity for recourse. Most instances leverage simple email spoofing, where a generic email is disguised to look like it is coming from the executive. Reputable email security software (that is correctly configured) will block spoofed emails. To avoid this, hackers are starting to invest time and effort to secure direct access to the executive's email account. We have seen examples of brute force attacks (guessing passwords) on the email account and tailored phishing attacks used to manipulate the executive to disclose their email password. When access to the email account is established, the hacker will monitor conversations, learn the executive's language and tone, and send targeted emails requesting logical payments be made by finance departments or personal accountants. These requests are difficult to distinguish from genuine requests. While most whaling attacks focus on fraudulently securing electronic fund transfers, we expect to see this method used more to illegally secure confidential information and to gain access to other systems. Ways to combat whaling attacks:

Create a business process that requires multiple confirmations or verbal confirmation on all payments over a predefined amount. This may be \$1000, or \$100,000. We have seen whaling attempts that were for small amounts (that we believe are test runs), followed by requests for much larger amounts.

Develop systems to protect information and access to other systems.

Educate staff, associates and executives on whaling attacks and how to address them. The more people know about social engineering methods, the more likely they are to spot the attacks.

Use a different password for your email account – do not use the same password for other accounts or site registrations (if you do, you are effectively handing over access to your email account).

Ensure your email security and firewalls are next-generation. Spoofed emails won't get through a strong email security posture.

For more information on email security, firewalls and educating staff on security threats and social engineering, contact your blueAPACHE Account Manager .

Related

[emPOWER Security](#)

[emPOWER Security \(pillar hub\)](#)

[Human Risk Management](#)

[Managed Detection and Response](#)

[blueAPACHE Security \(case study\)](#)

Frequently asked questions

What percentage of organisations saw an increase in targeted whaling attacks around the festive season, per the research cited in this post?

The post cites research showing 55 percent of organisations saw an increase in targeted whaling attacks around the festive season.

What is the most popular whaling attack type, and how often does it occur, according to the post?

The post says domain-spoofing is the most popular attack type, occurring in 70 percent of attacks.

How does this post define a whaling attack?

The post defines a whaling attack as a malicious email pretending to be from senior executives that requests finance employees make payments from company accounts to hackers' accounts.

How do more sophisticated hackers gain direct access to an executive's email account, per the post?

The post describes seeing brute force attacks that guess the executive's password, as well as tailored phishing attacks used to manipulate the executive into disclosing their email password.

What test-run pattern does the post describe in some whaling attempts?

The post says it has seen whaling attempts for small amounts, believed to be test runs, followed by requests for much larger amounts.

What five measures does the post recommend to combat whaling attacks?

The post recommends requiring multiple or verbal confirmation on payments over a predefined threshold, developing systems to protect information and access to other systems, educating staff and executives on whaling and social engineering, using a different password for the email account than for other services, and ensuring email security and firewalls are next-generation.

What does reputable, correctly configured email security software block, according to the post?

The post says most whaling instances leverage simple email spoofing, and that reputable email security software, correctly configured, will block these spoofed emails.

What future trend does the post predict for whaling attacks beyond fraudulent fund transfers?

The post says that while most whaling attacks currently focus on fraudulently securing electronic fund transfers, it expects the method to be used more to illegally secure confidential information and gain access to other systems.

Source

origin post (2016)

Knowledge Base

What is a whaling attack according to your blog?

In its simplest form, a whaling attack is a malicious email pretending to be from senior executives that requests finance employees make payments from the company accounts to hacker's accounts. It is also known as spear phishing and is a more targeted and purposeful version of phishing emails, often complete with footers and corporate branding that reflect the language and tone of the person being impersonated.

What percentage of organisations reported an increase in whaling attacks around the festive season, according to the blog?

Recent research cited in the blog shows that 55 percent of organisations have seen an increase in targeted whaling attacks around the festive season.

How do more sophisticated whaling attackers operate?

For more focused and intelligent attacks, hackers research the target business to identify its corporate structure, then use social engineering to manipulate people into wiring funds to bank accounts. Once payment is made, the money is quickly withdrawn or transferred elsewhere, leaving little opportunity for recourse.

How do hackers try to bypass email security software that blocks spoofed emails?

Since reputable, correctly configured email security software will block spoofed emails, hackers invest time and effort to secure direct access to the executive's actual email account. This includes brute force attacks (guessing passwords) and tailored phishing attacks used to manipulate the executive into disclosing their email password. Once access is gained, the hacker monitors conversations, learns the executive's language and tone, and sends targeted payment requests that are difficult to distinguish from genuine ones.

Besides fraudulent fund transfers, what other risk does the blog say whaling attacks may increasingly be used for?

The blog states that while most whaling attacks focus on fraudulently securing electronic fund transfers, it expects this method to be used more to illegally secure confidential information and to gain access to other systems.

What business process do you recommend to combat whaling attacks involving payments?

We recommend creating a business process that requires multiple confirmations or verbal confirmation on all payments over a predefined amount, such as \$1,000 or \$100,000, noting that some whaling attempts start with small test-run amounts followed by requests for much larger sums.

What are the recommended ways to combat whaling attacks listed in the blog?

The blog lists five ways to combat whaling attacks: 1) create a business process requiring multiple or verbal confirmations for payments over a predefined amount; 2) develop systems to protect information and access to other systems; 3) educate staff, associates and executives on whaling attacks and how to address them; 4) use a different password for your email account rather than reusing passwords across other accounts; and 5) ensure email security and firewalls are next-generation, since spoofed emails won't get through a strong email security posture.

Who should be contacted for more information on email security and staff education against whaling attacks?

The blog advises contacting your our Account Manager for more information on email security, firewalls, and educating staff on security threats and social engineering.