GreatHorn

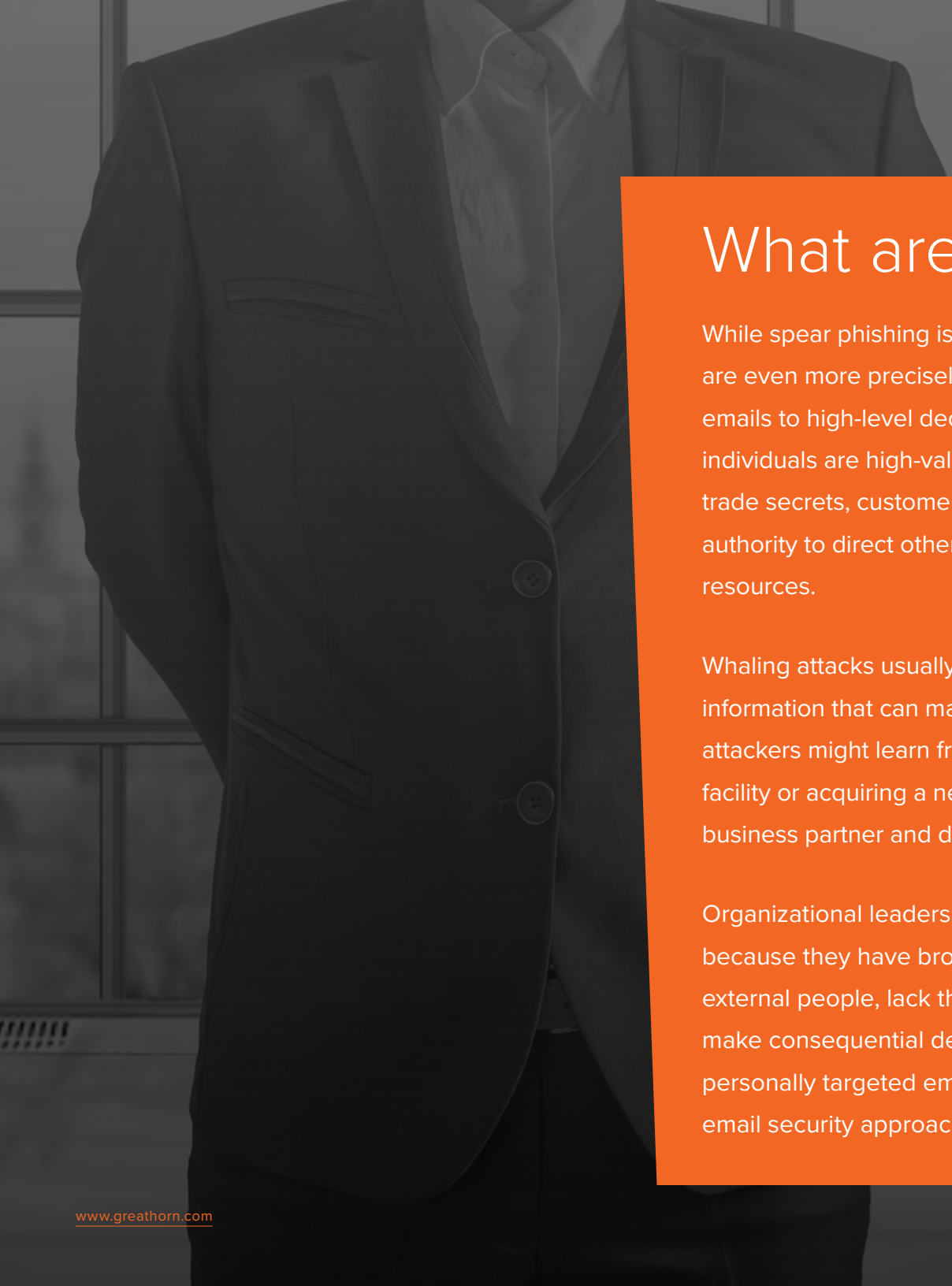
Get the facts on ...

Whaling Attacks

The latest trend in email attacks? Going after the "big fish" in your organization. Here's what you need to know to protect your enterprise from cybersecurity threats that target executives.

EBOOK

May 2021



What are Whaling Attacks?

While spear phishing is a highly targeted form of phishing, whaling attacks are even more precisely aimed. In whaling attacks, attackers send deceptive emails to high-level decision makers such as CEOs and CFOs. These individuals are high-value targets, because they typically have access to trade secrets, customer information and financial accounts. They also have authority to direct others in the organization to access and share these resources.

Whaling attacks usually begin with careful reconnaissance to gather relevant information that can make cybercriminals appear legitimate. For example, attackers might learn from news reports that a company is building a new facility or acquiring a new subsidiary. They can then pose as a vendor or business partner and direct the CFO to transfer funds to a fraudulent account.

Organizational leaders are uniquely vulnerable to such phishing attacks because they have broad responsibilities, interact with a wide range of external people, lack the time to carefully vet every email, and regularly make consequential decisions. And because whaling attacks involve personally targeted emails to carefully researched individuals, traditional email security approaches often fail to identify and stop them.

Data and Trends

59%

Of organizations say an executive has been the target of a whaling attack.

46%

Say executives have fallen victim.

68%

Are extremely or very worried executives will fall victim.

30%

Say whaling attacks have increased dramatically in the past year.

1 out of every 3,226

(Once every 24 Days)*

Emails received by an executive is a whaling attack*

Source: GreatHorn Surveys of 250 U.S. Cybersecurity Pros, March 2021
** Aggregated data from the GreatHorn Threat Intelligence Team*

Data and Trends

Use security awareness training to defend against whaling attacks.

Conduct awareness training at onboarding.

Conduct awareness training annually.

Source: GreatHorn Surveys of 250 U.S. Cybersecurity Pros, March 2021

Data and Trends

Have customized email security policies or rules for executives.

Ask executives to manually forward suspicious emails to the security team to address.

Source: GreatHorn Surveys of 250 U.S. Cybersecurity Pros, March 2021

Example Attacks

The GreatHorn Threat Intelligence Team assembled these examples of whaling attacks based on actual exploits.

Payment Routing Request

A typical whaling attack instructs a finance executive to route vendor payments to a new bank account. In this example, attackers have spoofed the email address of an employee at one of the victim's vendors. They establish legitimacy by referring to actual payment amounts and by copying actual employees of both the victim and the spoofed vendor. They also create urgency by following up on an earlier email and by suggesting that one of the victim's team members hasn't responded to an initial request.

From: McMurphy Carrie <carrie.mcmurphy@earthshakergroup.corn>
Date: Monday, March 20, 2021 7:20 AM
To: Judith Romano <jromano@sqpsales.com>
Cc: beth.schumann@earthshakergroup.corn; Mary Dallas <mdallas@sqpsales.com>
Subject: **External**ACH payment information update

Good Morning Judith,
Has our info been updated? Can we get a reply to our request below?

Let me know if there is anything you need.

Kind Regards,
Carrie McMurphy
Regional Credit Manager, Americas

Earthshaker Group
100 Meredith Hwy.
Norwalk, CT 06851 USA
Email: Carrie.McMurphy@earthshakergroup.com

From: McMurphy Carrie <carrie.mcmurphy@earthshakergroup.corn>
Date: Friday, March 17, 2020 10:51 AM
To: Judith Romano <jromano@sqpsales.com>
Cc: Beth Schumann; Mary Dallas <mdallas@sqpsales.com>
Subject: **External**ACH payment information update

Hi Judith,
We received the ACH payment of 358,481.55.

However due to ease of banking on our side, We are updating our ACH bank information to a more traditional US bank as i have tried explaining to Mary,

Attached is our payment instructions and update your records. You can let us know when you do so.

Let me know if there is anything you need.

Kind Regards,
Carrie McMurphy
Regional Credit Manager, Americas

Earthshaker Group
100 Meredith Hwy.
Norwalk, CT 06851 USA
Email: Carrie.McMurphy@earthshakergroup.com

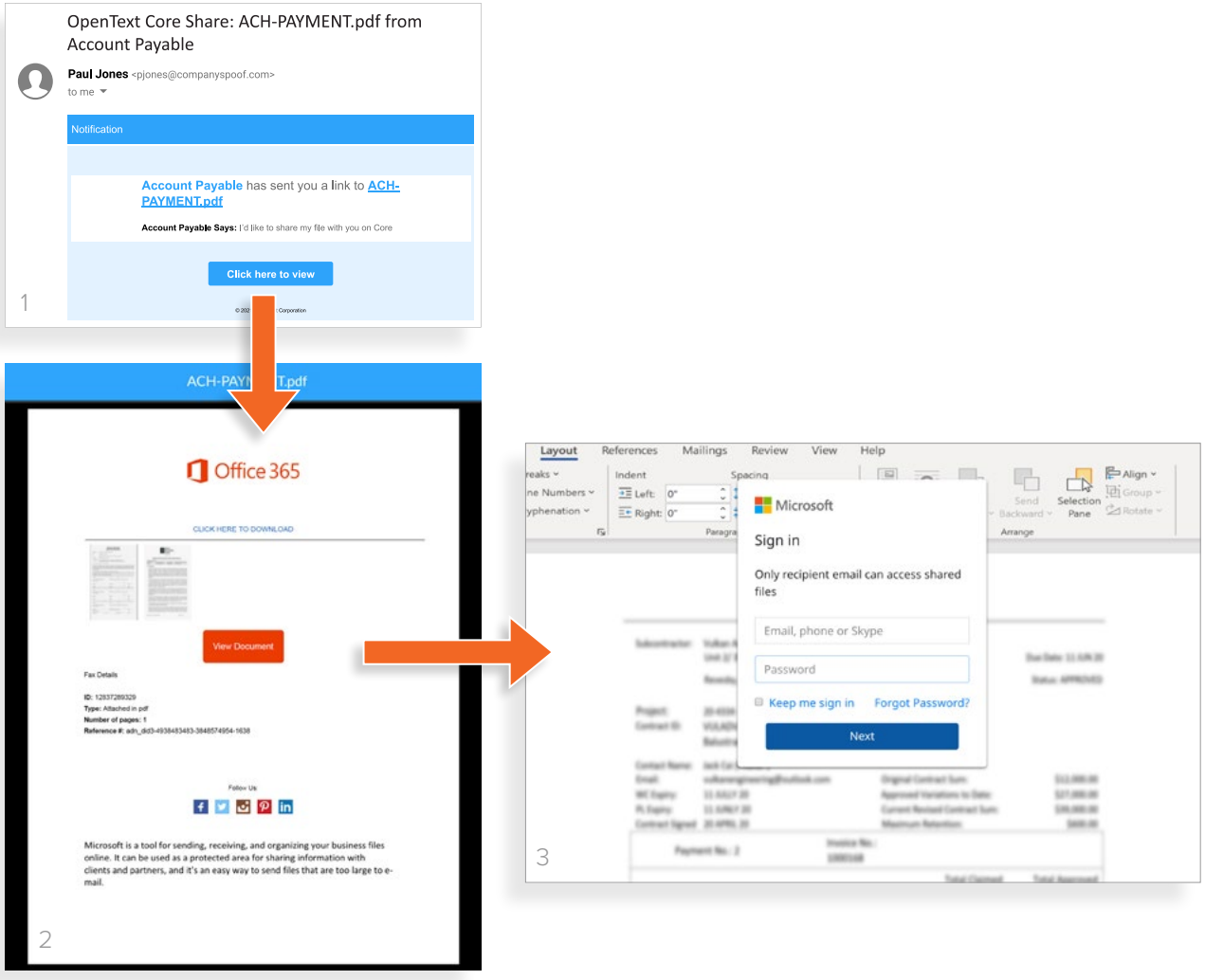
---

earthshakergroup.com

Example Attacks

Vendor Impersonation

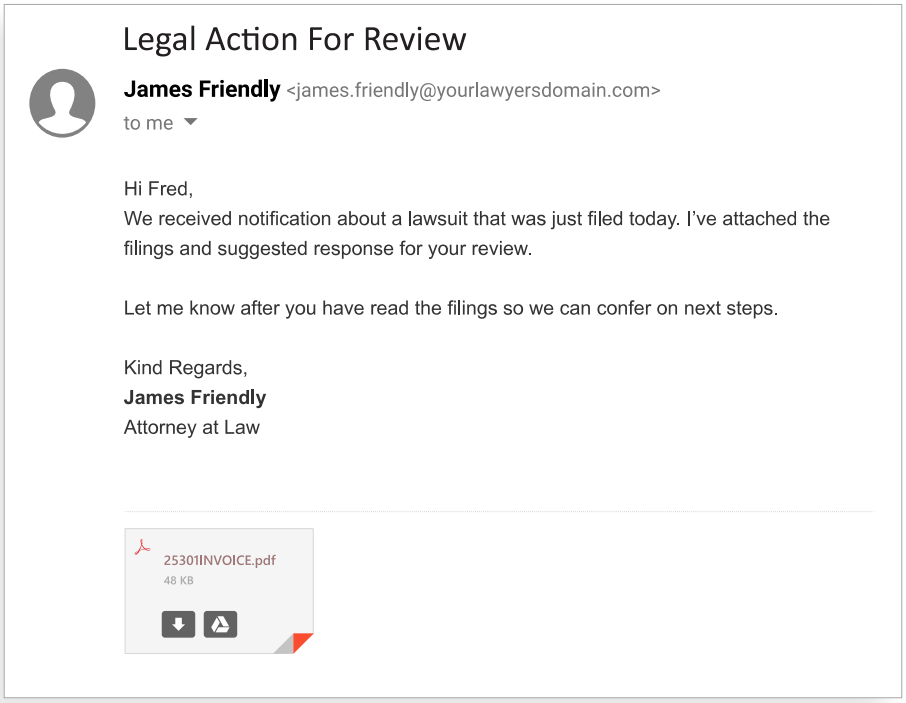
This two-step attack masquerades as a vendor requesting payment from the CFO. If the victim clicks on the embedded link, the email installs keylogging malware on the victim's system. When the CFO enters her Microsoft 365 username and password, the attacker captures the credentials.



Example Attacks

Business Lawsuit

In this common whaling exploit, attackers spoof the email address of legal counsel and send the CEO a malicious attachment about fake litigation. If the recipient clicks on the attachment, malware infects the corporate network.

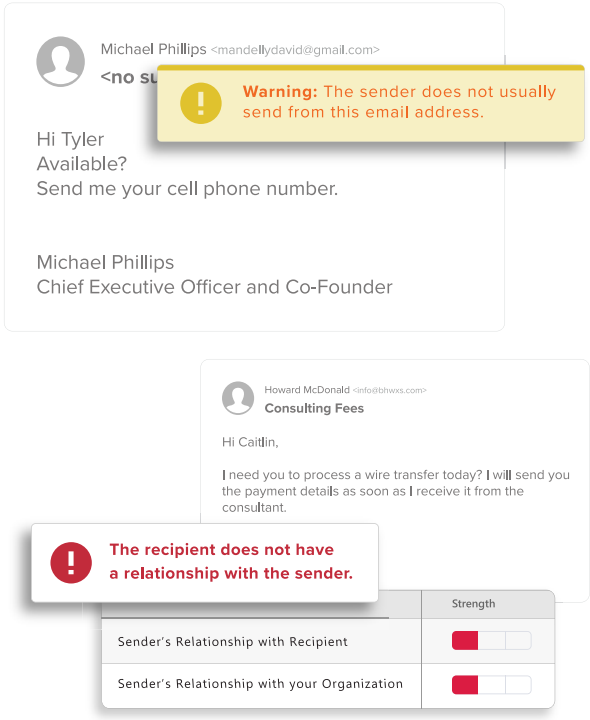


Actions You Can Take Today

Whaling attacks on organizational leadership are only increasing. But cybersecurity teams can take practical steps to minimize the risks these exploits present. Begin with clearly documented policies for executives and any employees who have access to financial systems. The email accounts of these individuals warrant stringent business rules, including filtering keywords commonly used in whaling attacks.

In addition, make sure your email security solution delivers the following functionality:

- **Behavioral Analytics**
  An effective email security solution should analyze all communication patterns between senders and recipients. It should apply artificial intelligence (AI) models and machine learning (ML) algorithms to provide immediate detection and insights into anomalous and potentially harmful email messages.
- **Relationship Strength**
  Your solution should evaluate email history to recognize and monitor the strength of every sender's individual relationship with every recipient across the enterprise. In addition, a "friends of friends" capability can account for a sender's overall relationship with others your organization.
- **Technical Fingerprints**
  The solution should offer sophisticated analysis of domain reputation, sending IP and header information. That evaluation must include determining variations in expected authentication results for Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).
- **Spoofing Likelihood**
  Robust analysis of employee display name spoofs, domain spoofs and domain lookalikes provides essential protections. The analysis should include comparison against known email addresses, executive impersonation tactics and email authentication standards.
- **Content Analysis**
  Deep content inspection can identify common spear phishing tactics – without storing an email message or its contents. Content analysis should be based on attachments, URLs, keywords and regular-expression (regex) search patterns. Spear phishing tactics content inspection can protect against include wire transfers, Form W-2 requests, credential-theft attacks and business-service impersonations.
- **Communication Patterns**
  Your email security solution should recognize communication patterns unique to your organization and to specific individuals within your organization – including email frequency, volume, recipients, sending behaviors and more.



Ready to reduce the risk of whaling attacks? Contact GreatHorn now to simplify your response to phishing attacks.

[6] *"Market Guide for Email Security," Gartner, September 2020*

About GreatHorn

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fast moving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.