Impersonation Protect

A Whale of a Tale: How to Stop the Rising Tide of Impersonation Attacks

mimecast® | making email safer for business

Impersonation Protect

A Whale of a Tale: How to Stop the Rising Tide of Impersonation Attacks

Whaling attacks have risen in recent months. In order to combat these attacks, organizations must be aware of the dangers presented by whaling, or CEO fraud, and put the right safeguards in place.

Whaling, its name derived from an analogy with a big 'phish', aims to target large enterprises for immediate financial gain and those who have access to key resources or functions within the business.

Cyber attackers have gained sophistication, capability and bravado in recent years, resulting is some complex and well-executed attacks. But, some of the most successful threat activity remains relatively basic, and uses simple social-engineering to dupe targets into transferring large amounts of money via wire transfer to criminal gangs.

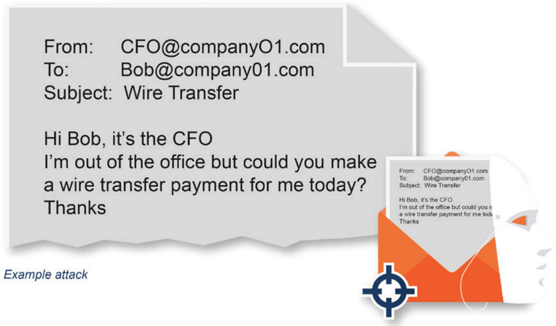
Mimecast conducted a whaling attack survey with 500 organizations globally in December 2015, and the results were alarming:

- 54.5% of organizations saw an increase in the volume of whaling attacks at the end of 2015.
- Domain-spoofing was the most popular attack vector (70%).
- 72% of whaling attackers pretended to be the CEO, while 35.5% were attributed to the CFO.

How Whaling Works

Whaling is a targeted attack, one that relies on a significant amount of prior research into a target organization, to identify the attacker's victim and the organizational hierarchy around them. Whaling attacks—like the one that hit US networking technology company Ubiquiti in 2015, resulting in $46 million in losses—use email sent from spoofed or similar-looking domain names. Emails appearing to be sent from the CEO or CFO are used to trick finance staff into making fraudulent wire transfers to the attackers. Whaling emails are more difficult to detect because they don't contain a malicious hyperlink or attachment, and rely solely on social-engineering to trick their targets.

For whaling to be so specifically targeted, the attackers research their victims to a much greater extent than usual. Social media provides attackers with much of the information they need; your company website combined with sites like Facebook, LinkedIn and Twitter provide key details that when pieced together give a much clearer picture of senior execs in the target organization.



From: CFO@companyO1.com
To: Bob@company01.com
Subject: Wire Transfer

Hi Bob, it's the CFO
I'm out of the office but could you make a wire transfer payment for me today?
Thanks

Example attack

Whalers do not need to use malware or have any technical expertise to exploit your organization. As a result the barriers to entry for this type of cyber-crime are painfully low. Using Ubiquiti as an example, we can see these attacks can be highly successful, especially for those organizations that are unprepared or unaware of the risks of such scams.

As whaling becomes more successful for cyber-criminals, we are likely to see a sharp increase in their prevalence, as hackers identify these attacks as highly profitable.

Anatomy of a Whaling Attack

Whaling can be easily broken down into five key phases.

1. **Attacker research.** Cyber criminals identify a target organization, and its employees—usually those who work in the finance department, as well as the C-Suite. They then leverage open source intelligence, social media, and corporate websites to build an accurate picture of the organization. Ultimately identifying the CEO, CFO and a very small number of individuals in the finance team.
2. **Similar-looking domain names.** Attackers may register a similar-looking or visually-similar domain name to their target company. For example the domain any-cornpany.com (note the use of R & N in place of M) could be used to spoof the legitimate domain, any-company.com. Occasionally if the organization doesn't yet own all the top-level domains (TLD) for its own domain. .net, .org, .int, etc. can be used effectively here.
3. **Attackers send 'phish' emails.** At this stage, the cyber-criminals will craft an email to a member of the finance team, impersonating the CEO or CFO, and using their newly-registered fake domain name. The email is typically well-structured, with correct grammar and spelling, making it look as innocuous as possible. Typically, the initial contact will be brief and to the point; something similar to, "I need you to complete a task ASAP, are you in the office?"
4. **Staff tricked by email.** For the attack to be successful, the victim must believe the email is genuine. Given the completeness of the research, it is extremely likely they will. When the finance team cooperates with the attacker, i.e. by replying to them, the attackers will pretend to be the CEO or CFO and will occasionally engage in email conversation with their victim. The ultimate payload is a request for a wire transfer to be made to a specific account, again established for the purposes of this attack.
5. **Wire transfer.** The finance team, when taken in by the attacker, are unaware of the scam and will use the information given to create a wire, bank or BACS transfer. Generally the attackers will target individuals with single sign-off approval for these sorts of transactions.

How to Protect Your Organization

In order to protect your organization from whaling, follow these simple steps:

- Educate your senior management, key staff members and finance teams on this specific type of attack. Don't include whaling in a general spear-phishing awareness campaign; single out this style of attack for special attention to ensure key staff remain vigilant.
- Carry out tests within your own organization. Simulate your own whaling attack as an exercise to see how vulnerable your staff are.
- Use technology where possible. Consider an inbound email stationery strategy that marks and alerts readers of emails that have originated outside of the corporate network.
- Consider subscribing to domain name registration alerting services, so you are alerted when domains are created that closely resemble your corporate domain. Consider registering all available TLDs for your domain, although with the emergence of generic TLDs this may not be scalable.
- Review your finance team's procedures; consider revising how payments to external third parties are authorized. Require more than single sign-off, or perhaps use voice or biometric approval only with the requestor to ensure validity of the request.

How Mimecast Can Help

In response to the growing threat of whaling, **Mimecast uniquely offers Impersonation Protect as part of its industry-leading Targeted Threat Protection service.**

Visit Mimecast.com to learn more about adding this vital service to your email security arsenal today.

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.