mimecast®

EMAIL SECURITY ADVISORY

Mimecast Warns of Heightened Whaling Threat

mimecast®

Mimecast has noted an increase in the prevalence of Whaling attacks on enterprises over the recent months; similar to the attack on Ubiquiti that resulted in $46 million in losses.

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. Or in other words, senior management. Cyber-attackers have gained sophistication, capability and bravado over the 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. Often transferring large amounts of money via wire transfer to criminal gangs for example.

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 of the type used at Ubiquiti and those that are increasingly popular, use email sent from spoofed or similar sounding domain names. Emails appearing to be sent from the CEO or CFO are used to trick finance staff into making illegitimate wire transfers to the attackers.

> **"WHALING IS SIMPLE FOR HACKERS TOO, WHO DO NOT NEED TO USE MALWARE OR ANY TECHNICAL EXPERTISE TO EXPLOIT YOUR ORGANIZATION. AS A RESULT THE BARRIERS TO ENTRY FOR THIS TYPE OF CYBER-CRIME ARE PAINFULLY LOW."**

Whaling emails can be more difficult to detect because they don't contain a hyperlink or malicious 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; sites like Facebook, LinkedIn and Twitter provide key details that when pieced together, give a much clearer picture of senior execs in the target business. LinkedIn for example can be used to map entire departments and reporting structures. Employees with excessively open social media profiles can be a rich seam of detail for these attackers, and those people will naturally be a point of call for cyber-criminals looking to exploit their employer.

Whaling is simple for hackers too, because they do not need to use malware or 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 a cash cow.

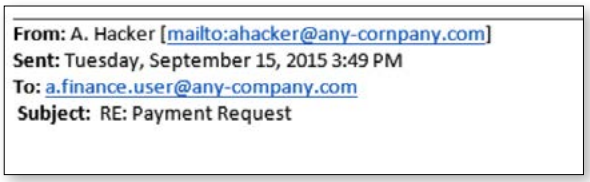
How Whaling Works

Whaling can be easily broken down into five key phases.

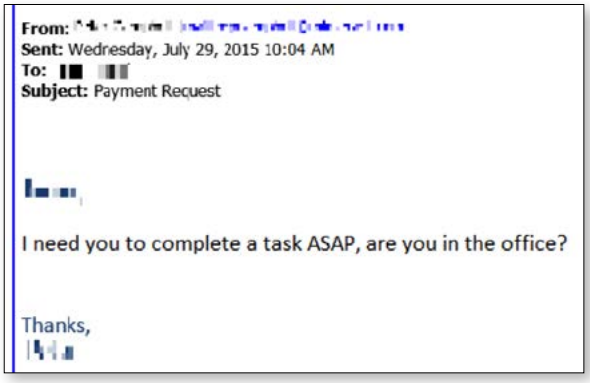
1. **Attacker research:** Cyber-criminals identify a target organization, and its employees—usually those who work in the finance department, as well as the C-Suite.

They then leverage open source intelligence (OSINT), 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.

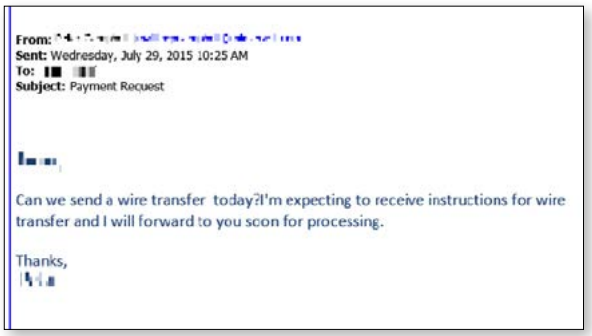
2. **Similar sounding domain names:** Attackers may then register a similar sounding or visually similar domain name to their target company. For example, the domain `any-cornpany.com` (note the use of R & N in place of M) could be used to spoof the legitimate domain, `any-company.com`. Occasionally if the organization doesn't yet own all the top-level domains (TLDs) 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, pretending to be from the CEO or CFO, 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 prior to the attack, success is usually highly likely. 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.



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.

> **"MIMECAST MONITORS THE GLOBAL PREVALENCE OF EMAIL BASED ATTACKS, LIKE WHALING AND SPEAR-PHISHING."**

Mimecast Recommendations

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 business. Build your own Whaling attack as an exercise to see how vulnerable your staff are.

> **"REVIEW YOUR FINANCE TEAM'S PROCEDURES; CONSIDER REVISING HOW PAYMENTS TO EXTERNAL THIRD PARTIES ARE AUTHORIZED."**

- Use technology where possible. Consider an inbound email stationery 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 (gTLD) this may not be scalable.
- Review your finance team's procedures; consider revising how payments to external third parties are authorised. Require more than single sign-off, or perhaps use voice or biometric approval only with the requestor to ensure validity of the request.

Mimecast 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.