BIZCOMMUNITY

Whaling attacks a heightened threat

Organisations are being warned of an increased prevalence of targeted whaling attacks, also known as Business Email Compromise - BEC.

Machado via pixabay

These attacks use email sent from spoofed or similar sounding domain names and appear to be sent from the CEO or CFO to trick accounting or finance users into making illegitimate wire transfers to cybercriminals. This type of targeted attack relies on a significant amount of prior research into a target organisation to identify the victim and the organisational hierarchy around them.

According to Mimecast research conducted in December 2015*:

• 55% of organisations have seen an increase in the volume of whaling attacks over the last three months
• Domain-spoofing is the most popular attack type (70%), while top-level domain squatting (e.g. mycompany.biz) is at 16%
• Most whaling attacks pretend to be the CEO (72%), while 35% had seen whaling emails attributed to the CFO
• Whalers also prefer Gmail accounts (25%) over Yahoo (8%) and Hotmail (8%)

Sophisticated social engineering

Orlando Scott-Cowley, cyber security strategist at Mimecast, commented: "Cyber attackers have gained sophistication, capability and bravado over the recent years, resulting in some complex and well-executed attacks. 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."

Social media provides attackers with much of the information they need to execute these attacks, especially when combined with wider insider research. 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.

Mimecast's whaling protection recommendations

• Educate senior management, key staff and finance teams on this specific type of attack

• Carry out tests within your own business. Build your own whaling attack as an exercise to see how vulnerable your staff are

• Use technology where possible. Consider inbound email stationery that marks and alerts employees to emails that have originated outside of the corporate network

• Subscribe to domain name registration alerting services so you are alerted when domains are created that closely resemble your corporate domain

• Consider registering all available top-level domains (TLDs) for your domain, although with the emergence of generic TLDs (gTLD) this may not be scalable

• Review your finance team's procedures and consider revising how payments to external third parties are authorized

"The barriers to entry for whaling attacks are dangerously low. As whaling becomes more successful for cybercriminals, we are likely to see a continued increase in their popularity, as hackers identify these attacks as an effective cash cow," added Scott-Cowley.

**Mimecast conducted a survey of 442 IT experts at organisations in the US, UK, South Africa and Australia in December 2015.*

Download Mimecast's whaling security advisory for a more detailed analysis, including a breakdown of how whaling attacks are conducted.