Business Email Compromise (BEC) in Action

One of the key indicators of phishing scams is they're typically random, unexpected messages. What if, however, an attacker managed to insert themselves into an ongoing communication thread? That's exactly what can happen if someone's email account gets hacked — a spear phishing attack known as business email compromise (BEC). Let's review how this works.

Research and Identify the Target

Unlike generic phishing scams, BEC attacks often involve thorough research of the target to ensure they are someone with access to finances or confidential information. The attacker will use any information they find to create personalized messages or phone calls designed to gain trust.

Launch the Attack

With trust established, the attacker can send an email containing a malicious link or attachment. Either of these can infect the device with malware (malicious software). Malware can steal passwords and give the attacker access to the email account.

Monitor Communications

If they get access, they can monitor communications between the target, their clients, and co-workers. The goal is to identify situations where wire transfers will be involved and when those transfers are expected to occur.

Hijack the Thread

As soon as it's clear that a payment is ready to process, the attacker will send a message, using the compromised email account, with updated (and fraudulent) payment instructions. Since the message comes from a trusted source in an ongoing communication, the victim usually has no reason to think it's suspicious.

This type of attack can result in significant financial loss or theft of highly confidential information. That's why it's vital to use caution when handling requests for money or information. Always verify a request is legitimate by reaching out to the sender through an alternative, trusted communication channel. Verify before you comply!