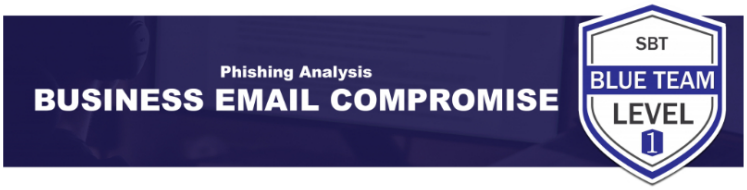
Business Email Compromise



A business email compromise is a very impactful attack, and can potentially lead to private information disclosure, or heavy monetary losses, depending on the actions that the malicious actor decides to take. This lesson will cover exactly what BEC is, and how they're so effective at evading email security systems.

WHAT IS B.E.C?

A business email compromise is a phishing attack that can target any organization, but focuses on those that are likely to transfer large amounts of money to either purchase goods or pay other parties such as vendors. The malicious actor will monitor their target over a period of time to determine which companies the organization pays, and when they have found a relationship between the company and a supplier, they will either compromise an email account belonging to a member of the executive board or a high-level employee, or spoof the address so it appears legitimate, and will instead direct the relevant employees to transfer the money to a different bank account that is under the malicious actor's control. This may seem like an easy attack to spot, but it works. Business email compromise attacks accounted for an estimated $1.77 billion of losses in the USA during 2019, as reported by the FBI. This is an incredible amount of money that has been lost by what is seemingly an "easy" attack to conduct. The more experienced and knowledgeable the malicious actors are, the better they can use social engineering principles to deceive the recipients of these malicious emails into providing malicious actors with information or transferring funds.

Below we will cover 5 different real-world scenarios where business email compromise is featured.

Email Compromise & Vendor Attack

In this scenario, a legitimate email account belonging to an employee who handles payments to vendors is compromised via credential stuffing, a key logger, or some other initial vector. The attack creates an invoice that is branded to look like it has come from the compromised organization (potentially even by retrieving legitimate invoices and editing the text). This will be sent out to any vendors that are in the address book of the compromised email account, and vendors will potentially pay into a malicious actor-owned bank account.

Email Spoofing & Alternative Payment Attack

In this scenario either a legitimate email account is compromised or the malicious actor will spoof an email address from the initial organization, and send an email to the target company, offering an alternative payment method for any future payment. If the vendor doesn't discover this is a spoofed email, they may pay any future payments into the malicious actor's bank account.

Email Spoofing & CEO Fraud

In this scenario, the malicious actor is posing as a member of the executive board, such as the CEO, CTO, CFO, etc, and either contacts employees in the finance department, or either the financial institution that the organization uses to hold their money. They use social engineering tactics to create a sense of urgency, and convince the employee they're communicating with, that they are in a time-sensitive situation and need money transferred to their bank (actually a malicious actor-controlled account) immediately.

Email Spoofing & Data Theft

Email Spoofing & Data Theft

Malicious actors will spoof an employee, and request to see what information is held on them or requesting tax invoices. This will allow the phisher to get detailed information about an employee, such as their home address, payment information, contact information, and more. This will typically be used for further spear phishing emails, as they will be extremely effective as they are using real information about the target. This information could also be sold on to other hackers so they can conduct further attacks themselves, such as blackmail or impersonation.

Email Compromise & Zombie Phishing

Zombie phishing is when a malicious actor compromises an email account, and replies to old email threads between one or more contact, and inserts a malicious URL into the email. This is more likely to be clicked, as it will have come from a sender that the recipients are familiar with, and have previous legitimate email communication with. This can be extremely effective if done right.

Previous Topic
Back to Lesson
Next Topic