What is vendor email compromise (VEC)?

Archived: 2026-04-05 23:45:54 UTC

What is vendor email compromise (VEC)?

Vendor email compromise, also referred to as “financial supply chain compromise”, is a targeted type of business email compromise (BEC) attack in which attackers impersonate a third-party vendor in order to steal from that vendor’s customers. Vendors often work with a variety of customers — by compromising and impersonating the vendor, attackers can persuade multiple targets to give up money or sensitive information.

What is business email compromise?

Business email compromise (BEC) is a type of social engineering attack that takes over the victim’s emails. In a BEC attack, the attacker falsifies an email message through plain text to trick the victim into a predetermined set of actions, such as revealing sensitive data.

BEC is notable in that it often targets a specific individual within an organization. BEC is often difficult to detect. The emails can easily go unnoticed by traditional email security solutions because they do not contain malware, malicious links, dangerous email attachments or other elements the email security solution uses to filter and identify phishing emails. BEC emails use plain text carefully designed and crafted to trick the recipient and to avoid existing security techstack. The emails are typically phrased in a way that mimics the tone and content of trusted senders such as coworkers or CEO, which helps trick the recipient into engaging with them.

While vendor email compromise attacks are a type of BEC attack, they are not necessarily the same. A typical BEC attack campaign targets a personal or executive to obtain confidential information, while a vendor email compromise campaign typically requires a greater understanding of existing business relationships, such as payment structures, financial information and existing vendor-client processes. The research process of a vendor email compromise may take weeks to months and the potential payoff for the attacker is far greater.

How do vendor email compromise attacks unfold?

Vendor email compromise attacks are sophisticated, complex, and hard to detect. They can take months, if not years, to design, infiltrate, and fully implement. However, there are common steps to every vendor email compromise attack:

1. **Conduct in-depth research on the vendor and their client base.** Using publicly available information, attackers will learn about their target vendor’s employees, customers, work processes, billing cycles, and other facts. This process may take weeks or months to complete, but the research ultimately helps the attacker impersonate the defender more convincingly
2. **Sending phishing emails to the vendor.** Before carrying out attacks against their final targets, attackers must first obtain access to the targeted vendor’s email account. To do this, attackers often send several phishing emails to the vendor that contain malicious links.

3. **Take over the compromised account.** Once attackers gain access to the vendor's email account, they create email forwarding rules to send relevant email copies to the attacker's inbox. From here, the attacker will monitor the inbox for pertinent financial information such as bank account, invoice details, and payment schedules.
4. **Send targeted vendor email attacks to the vendor's customers.** The last step is to design a highly sophisticated and hard to detect spear phishing campaign email to the vendor's customers, typically around the time of billing. Using the information gleaned from the research phase, attackers typically try to persuade their victims that they owe the vendor money, and to send the supposedly 'required payment' to the attacker's account.

What are the consequences of a vendor email compromise attack?

Vendor email compromise campaigns affect two different victims — the compromised vendor, and the vendor's customers or suppliers.

Compromised vendors may experience reputational damage and financial losses in the form of misdirected payments. The attacker can gain access to funds meant for the vendor by redirecting client payments to an attacker specified account. And once the attack campaign is discovered, the vendor's reputation may take a hit due to fears that an existing or potential client's private data will be exposed.

In addition, the "final" targets – the clients or suppliers targeted from the compromised vendor account – may suffer steep financial losses, loss of service, and a jeopardized supply chain.

One example of a vendor email compromise attack is the December 2020 attack on nonprofit One Treasure Island. Attackers impersonated a third-party bookkeeper, infiltrated existing email chains, and sent a payment transfer request email with alternative wire transfer instructions. One Treasure Island staff member transferred a large payment meant for the partner into the attacker's account, losing $650,000. This attack led to financial losses, loss of service and a jeopardized vendor for One Treasure Island, and reputational and financial loss for the compromised third-party bookkeeper.

How can Cloudflare prevent vendor email compromise?

Cloudflare Email Security protects against a wide range of attacks, including preventing sophisticated and hard-to-detect targeted vendor email compromise campaigns. This advanced email protection is powered by Cloudflare's global network, which blocks an average of 86 billion threats a day. As part of the Cloudflare SASE platform, it helps provide continuous, comprehensive security and makes it easy for vendors and organizations to enforce secure, cloud-native, on-premise security solutions.

FAQs

What is vendor email compromise (VEC)?

Vendor email compromise, also known as financial supply chain compromise, is a sophisticated and targeted type of business email compromise (BEC) attack. In a VEC attack, an attacker impersonates a third-party vendor to

trick that vendor's customers into sending money or sensitive information to the attacker.

How does a vendor email compromise attack work?

These attacks are multi-staged and can take months to execute. First, the attacker conducts in-depth research on the target vendor and their clients. Next, the attacker has to successfully phish the vendor to take over their account. Once inside the vendor's email account, the attacker sets up forwarding rules to monitor financial information, like invoices and payment schedules. Around a billing cycle, the attacker uses the compromised account to send spear phishing emails to the vendor's customers.

What are the consequences of a VEC attack?

A VEC attack impacts both the compromised vendor and their customers. The vendor can suffer significant reputational damage and financial loss from misdirected payments. The vendor's customers can also face steep financial losses, service disruptions, and a jeopardized supply chain.

How can organizations prevent vendor email compromise?

Advanced email security solutions can protect against these sophisticated attacks. For instance, Cloudflare Email Security uses its global threat intelligence network to detect and block VEC campaigns. This type of solution can be part of a broader zero trust security platform that provides comprehensive protection for an organization's cloud and on-premises systems.

How is VEC different from BEC?

Vendor email compromise (VEC) is a type of business email compromise (BEC) attack. However, a VEC attack often has more layers to it than a typical BEC attack. A BEC attack may directly target a business or an individual, while a VEC attack first targets a vendor, then targets the vendor's customers.
