Courtesy of
SCS Agency Inc

Vendor Email Compromise

Businesses increasingly rely on their vendor relationships for operational continuity and long-term growth. Yet, this trusted business-vendor relationship can be exploited by cybercriminals. Vendor email compromise (VEC), also known as supply chain compromise, is a rapidly growing email threat that can deceive even the most security-conscious employees.

In VEC attacks, threat actors impersonate trusted business partners or suppliers via email to disrupt operations, gain unauthorized access to systems, steal sensitive data or divert payments. Unlike traditional business email compromise (BEC) scams, which more commonly impersonate internal executives or employees, VEC attacks focus on external partners, vendors and suppliers.

This article examines the risks associated with VEC attacks, explores why VEC scams are successful and outlines strategies for combating this growing threat.

Understanding Vendor Email Compromise Risks

VEC attacks use personalization and social engineering tactics to exploit the trust established between businesses and their vendors. Many employees have grown savvy to the tactics used in traditional phishing emails, such as generic subject lines, suspicious links or poor grammar. However, VEC attacks mimic legitimate vendor communications, making them more difficult to detect. In fact, companies may not even realize they have been targeted until money or data has gone missing.

A typical VEC attack may occur in the following manner:

1. **Initial compromise**—Cybercriminals gain access to a vendor's email account using a range of approaches. Common breach tactics include sending traditional phishing emails containing malicious links and credential stuffing, where stolen login details are tested in bulk against vendor email systems. Alternatively, malicious actors may use lookalike domains to pose as the vendor.
2. **Information gathering**—Cybercriminals conduct in-depth research and reconnaissance over weeks or months. They analyze the vendor's interactions with its customers and partners through public information and social media, collecting sensitive details such as account information, payment schedules and the identities of individuals who authorize payments.
3. **Account takeover**—Attackers establish forwarding rules within the compromised vendor email account, secretly diverting copies of all incoming and outgoing messages to their own inbox. This allows them to harvest additional sensitive information without detection.
4. **Attack execution**—Threat actors launch highly sophisticated, targeted email campaigns aimed at the vendor's clients, often directed at specific employees responsible for authorizing payments or managing accounts. Using terminology and communication patterns gathered during reconnaissance, these emails may request updated banking details or credential verification.

VEC attacks can have a significant impact on affected organizations. Clients of compromised vendors may face supply chain disruptions, financial losses and operational setbacks. Vendors themselves risk financial and reputational damage, as customers may switch to

SCS AGENCY INSURANCE

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

competitors due to fears that their data has been exposed. Beyond these immediate effects, VEC attacks may trigger regulatory investigations, lawsuits and potential fines for noncompliance with data protection laws. They may also erode long-standing business relationships, weaken trust across the supply chain and create lasting brand damage.

Why VEC Attacks Succeed

VEC attacks succeed by exploiting human trust in subtle ways. Unlike traditional BEC scams, where attackers typically pose as company leaders making unusual requests (e.g., wire transfers), VEC attacks exploit the routine nature of vendor communications, making fraudulent requests appear legitimate and convincing. Because employees are accustomed to regular conversations with vendors about invoice changes, payment updates and contract modifications, these attacks are more difficult to spot.

Additionally, red flags often apparent in fraudulent emails may be absent. For example, the email's "To" and "From" fields may appear correct if the vendor's email account was compromised, and the timing may align with scheduled payment runs due to prior reconnaissance.

Moreover, traditional email defenses are often insufficient to detect and stop such sophisticated socially engineered attacks. Email gateways typically flag suspicious links, malicious attachments or domain spoofing, indicators that may be absent in VEC scams.

Prevention and Mitigation Strategies

To mitigate the risks of VEC attacks, organizations should consider the following proactive strategies:

- **Implement technical safeguards**. Organizations should implement advanced email authentication protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), to verify sender identity and block VEC attempts that rely on fake or spoofed domains. However, because many VEC attacks stem from legitimately compromised vendor mailboxes, these controls should be paired with additional behavioral and access-based defenses.
- **Deploy behavioral monitoring tools**. Organizations should consider utilizing modern behavioral monitoring tools to flag suspicious emails. Such tools utilize artificial intelligence to analyze communication patterns, detect anomalies and identify emails that deviate from regular vendor or employee behavior.
- **Establish vendor verification procedures.** Organizations should verify any vendor requests that involve sensitive data, money or account changes before proceeding. For instance, employees could use secure portals or phone vendors directly before acting on payment requests. Vendors should also be required to use secure, authenticated email channels and provide regular updates on their security controls.
- **Monitor the security posture of vendors**. Organizations should continuously assess and monitor the security posture of vendors, including whether they have been the subject of breaches. Vendor risk management tools can provide timely visibility and help streamline this process.
- **Train staff to recognize VEC tactics**. Organizations should provide role-specific, scenario-based training to educate employees on VEC tactics, warning signs and the importance of pausing and verifying suspicious requests or payment update notifications.

Adopting a multilayered approach to email security is the most effective way to defend against sophisticated threats, such as VEC attacks.

Insurance Response to VEC Attacks

Both cyber and crime insurance policies can provide coverage for direct financial losses stemming from fraudulent fund transfers, invoice manipulation and payment diversion. However, coverage depends on a policy's specific wording. Some policies may only be triggered by a direct breach of system security and may not extend to situations where employees are misled into taking fraudulent actions, such as authorizing payments in VEC attacks. Some policies may not respond when employees voluntarily send funds unless specific social engineering or fraudulent instruction endorsements are in place. In many cases, commercial crime policies endorsed for social engineering fraud are better suited to covering direct financial losses from fraudulent payment instructions. In contrast, cyber policies often address incident response costs, data exposure and regulatory liabilities.

Working with an experienced insurance broker can help in this regard. Brokers can check that cyber and crime insurance policies complement each other, identify coverage gaps and suggest specific endorsements (e.g., social engineering fraud) to ensure robust financial protection against VEC attacks and other deception-based threats. Brokers can also support organizations throughout the claims process, potentially helping to achieve faster resolution of coverage determinations and claim settlements.

Conclusion

As organizations increasingly rely on wider supply chains to grow their operations, they also face greater exposure to vendor risks, including VEC attacks. Organizations can enhance their resilience to these and other attack types by implementing robust risk-mitigation measures and reviewing their insurance policies.

Contact us today for additional risk management and insurance solutions.