Understanding Vendor Fraud and Supply Chain Risk
Executive Summary

Interacting with vendors has become an everyday part of doing business. And through these frequent interactions, many of us build a certain level of trust with our vendors over time. Sadly, bad actors are counting on this trust, eager to exploit it. For organizations that work with vendors and suppliers, it is important to take the necessary precautions to protect your organization against vendor fraud and supply chain attacks.

According to the 2022 Email Security Threat Report, the Armorblox research team saw a 73% increase in financial fraud email threats year-over-year from 2021 to 2022. And 44% of these financial fraud attacks were sophisticated, targeted attacks such as wire fraud, invoice fraud, or vendor fraud.

Does your Current Email Security Solution Identify Vendor Fraud Attacks?

Businesses that transact with vendors to supply products or services are at risk of Vendor Email Compromise, also known as Vendor Impersonation Fraud. The attacks are sophisticated and once attackers compromise a trusted vendor or third party contact, your business is at risk. Successful VEC attacks can inflict widespread damage to a business, its partners, customers, and other key stakeholders, resulting in sensitive and confidential data loss, financial loss, and/or reputational burden.

In order to prevent these sophisticated email attacks, organizations must employ an email security solution that leverages language signals to identify and track vendor communications and vendor-related business workflows. Email security solutions that provide this sophisticated level of monitoring are key to protecting organizations against targeted vendor fraud and supply chain attacks. These capabilities allow for preventative protection against misaddressed vendor communications, fake invoices, and zero-day phishing attacks.

Three Types of Vendor Fraud Attacks

Bad actors deploy three main types of tactics across targeted vendor fraud attacks. These include creating legitimate domains to bypass incumbent security tools, spoofing trusted vendor contacts, or through a takeover of a vendor or third-party contact’s account.

1. Look-alike Domains

Bad actors register look-alike domains aimed to impersonate companies to leverage the credibility of well-known brands. Intentionally misleading, look-alike domains can provide victims a false sense of trust that they are interacting with a legitimate brand; oftentimes leading to the exfiltration of user credentials or sensitive business data. For example, walmart.com and waImar t .com (the second one has an upper case i instead of a lowercase L - easily missed by the human eye.)
2. Header Spoofing

With header spoofing, an attacker uses mail services like SendGrid or other providers to spoof the mail header to make it look like the mail came to the user from an individual or brand that they know or trust. In these attacks, bad actors forge email headers so that email software displays the fraudulent address of the sender. If victims see a name that they recognize, they are more likely to engage with and trust the email came from a legitimate source. This can lead to unsuspecting victims clicking on malicious links within the email body or attachments, opening malware attachments, or sending sensitive data.

3. Account Compromise

An account compromise happens when bad actors gain access to legitimate accounts in order to exfiltrate data, steal credentials, or for financial gain. When vendor accounts are compromised, these takeovers result in bad actors hijacking business email workflows for a variety of vendor or supplier-related communications.

How Bad Actors Look to Exploit Vendor Business Workflows

There are several vendor business workflows that bad actors look to exploit, and preventing these workflows from compromise requires language-based email security solutions. Compromised email workflows can include hijacking email threads, sending documents that require logins, and using compromised accounts to steal wire transfer payments. A language-based email security solution like Armorblox utilizes AI, natural language understanding, and machine learning to understand the context and content of these communications, protecting you against these attempts.

After a successful account takeover, bad actors aim to exploit everyday vendor-related business workflows that mimic communications commonly exchanged with trusted vendors, such as:

- Sending an email from the compromised vendor account with information on a new distribution list or email address that must be used for all subsequent communications, resulting in all ongoing communications going directly to the bad actor’s preferred email address.
- Sending a link to documents that requires a login to view, leading to sensitive user credentials being compromised.
- Hijacking an email thread regarding an invoice awaiting payment with updated bank number and account information, resulting in payment fraud as soon as the payment is successfully sent to the bad actor’s personal bank account.
- Sending an email from the compromised vendor account containing new instructions for wire transfers, leading to wire fraud and all subsequent payments being made directly to the bad actor versus the legitimate vendor.
Why Traditional Cybersecurity Solutions Fail to Detect Vendor Email Fraud

Traditional cybersecurity solutions fail to catch targeted, vendor fraud attacks because:

• Detecting a suspicious login attempt or IP address are small signals that usually don’t warrant standalone enforcement policies.
• Detecting look-alike domains inside a protected organization is easy, whereas the detection of look-alike domains outside of the organization is much more difficult.
• Reading and analyzing the content and context of an email exchange is a manual process. Only an NLU platform trained on a large, accurately-labeled dataset can automate this process. Additionally, the platform would have to constantly retrain and easily classify what’s important, which is no easy feat.

Vendor Email Compromise can be difficult to detect and prevent, putting organization-specific sensitive data and finances at risk. Protecting your company against vendor email fraud can be challenging, but consistently using the right strategies and tools can help defend your reputation, vendor relationships, and, ultimately, your bottom line.

Use the checklist below to assess your organization’s needs in a security solution that can protect against vendor email compromise and supply chain attacks.

<table>
<thead>
<tr>
<th>REQUIRED</th>
<th>NICE-TO-HAVE</th>
<th>IN PLACE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous vendor identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor risk assessment based on threat history</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor business workflow identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor communication monitoring across the organization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language-based models that identify fraudulent vendor requests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global models that track vendors across all customers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation of credential phishing attempts from compromised vendor accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Armorblox

Armorblox secures enterprise communications over email and other cloud office applications with the power of Natural Language Understanding. The Armorblox platform connects over APIs and analyzes thousands of signals to understand the context of communications and protect people and data from compromise. Over 58,000 organizations use Armorblox to stop BEC and targeted phishing attacks, protect sensitive PII and PCI, and automate remediation of user-reported email threats. Armorblox was featured in the Gartner 2021 Market Guide for Email Security and Gartner 2022 Market Guide for Data Loss Prevention.


Schedule a live demo with one of our email security experts today: visit, https://get.armorblox.com/demo

⭐⭐⭐⭐⭐

Inboxes That Love Armorblox

“Since implementing Armorblox, we've been able to protect not only Intermedia's corporate users but also over one million customers. We are a hosted Microsoft Exchange Provider and Armorblox was the only partner who could help us protect our on-premise mailboxes and was the only decision for our team."

JONATHAN LEVINE, CTO, INTERMEDIA CLOUD COMMUNICATIONS

"What is really neat for me as a CIO is that whenever I get an email that looks suspicious, I forward it to the email abuse mailbox. Armorblox then immediately quarantines the threat for everybody else. As soon as that happens, the magic starts."

HOWARD MILLER, CIO, UCLA ANDERSON SCHOOL OF MANAGEMENT