Abnormal SECURE|ANCHOR

CISO Guide to Vendor Email Compromise

Stopping the Vendor Fraud Attacks That Exploit Trusted Partnerships

/ By Dr. Eric Cole
Founder and CEO, Secure Anchor

The Rising Threat of Vendor Email Compromise

Vendor email compromise (VEC), also referred to as supply chain compromise, is a significant security threat to enterprise organizations. This form of attack occurs when a threat actor gains control of a vendor email account and then uses it to steal money from known contacts. VEC attacks are highly successful because they exploit trusted communications between vendors and customers through personalization and social engineering.

According to research from Abnormal Security, two-thirds of large enterprises experienced a VEC attack in Q4 2022. Threat actors increasingly see communications between vendors and customers as the weakest link. Once they gain access to vendor accounts, it becomes easy to focus their efforts on VEC attacks, as they are much more lucrative than traditional scams.

It's clear traditional email defenses were not designed to stop socially-engineered attacks. Without a new approach, high-profile attacks such as SolarWinds and Colonial Pipeline, which we can surmise started with socially-engineered vendor fraud campaigns, will continue to cause severe financial losses and reputational damage.

67%

percentage of large enterprises that experienced a VEC attack in Q4 2022.

Types of Vendor Email Compromise Attacks

Vendor email compromise is not a monolithic type of attack and can take on many forms. Here are a few of the ways attackers leverage compromised accounts to steal money from organizations.

Invoice Fraud

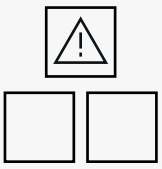
The attacker uses the compromised account to send a fraudulent invoice. In many cases, this looks exactly like a real invoice and even includes the expected billing amount, as the attacker has access to the entire email account and can research past conversations. Typically, the only difference is that the banking details have been changed to an account in the attacker's control.

Billing Account Update Fraud

Using the compromised account, the attacker sends a notice about a recurring payment or outstanding invoice, indicating that the recipient must update payment details to an account under their control. These attacks use similar phrases like "bank reconciliation audit" and needing to send money to a "secondary bank account."

Payment Fraud

Payment fraud is defined as any compromised vendor email account that attempts to steal money and/or goods from a target through means that don't involve a specific invoice or payment transaction. Payment fraud attacks can take different forms, including RFQ scams, aging report scams, or invoice inquiries, where the attacker asks for details about an upcoming payment.



RFQ Scams

An RFQ scam starts with the attacker emailing the supplier for a specific set of merchandise. After the vendor responds, an official-looking purchase order is then delivered containing the logo, contact information, and most importantly, the delivery information for where the goods are to be shipped. Attackers will often use the real information of companies they have compromised in order to pass credit checks so they can receive the goods on credit. If successful, this concludes with the goods being shipped to the attacker (rather than the compromised vendor) and no payment is made for the goods in question.

It's worth noting that vendor email compromise attacks can take many other forms and often do. These attacks can be part of larger credential phishing or account takeover schemes and can have dire consequences for both organizations involved.

Abnormal SECURE|ANCHOR

Impact of Vendor Email Compromise Attacks

The FBI's Internet Crime Complaint Center (IC3) actively tracks financial losses from business email compromise (BEC) attacks, of which vendor email compromise is part. The 2020 Internet Crime Report revealed that BEC crimes cost businesses $1.86B, with an average of $96,000 per complaint. This data, however, is based on complaints after attacks were successful.

Abnormal has found that the impact of VEC is much higher than the average BEC attack—likely because these attacks utilize compromised accounts and are thus much harder to detect.

$183K

The average cost of a vendor email compromise attack is $183,000.

$300K

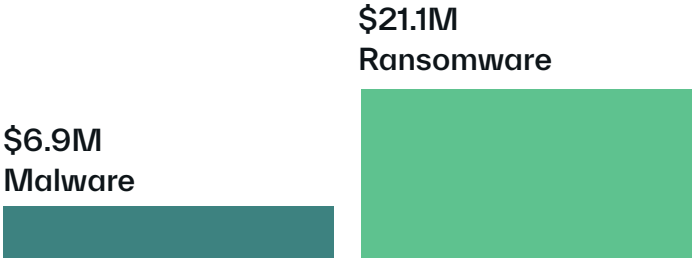
Billing account update fraud is the costliest form, accounting for an average of $300,000 per attack.

$120K

The average potential cost of invoice fraud is $120,000, with a maximum identified attack of $466,000.

Socially-Engineered Attacks are the #1 Security Threat

2020 FBI IC3
Jan 2021



$2.1B
Socially-Engineered Attacks

BEC/EAC | Spoofing | Phishing

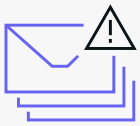
Abnormal | SECURE|ANCHOR

Why Vendor Email Compromise Attacks are Successful

To stop vendor email compromise, there needs to be a fundamentally different approach to the problem. The old approach relies on threat intelligence as a means of detecting and preventing all attacks. Unfortunately, threat intelligence has known limits to what it can stop.

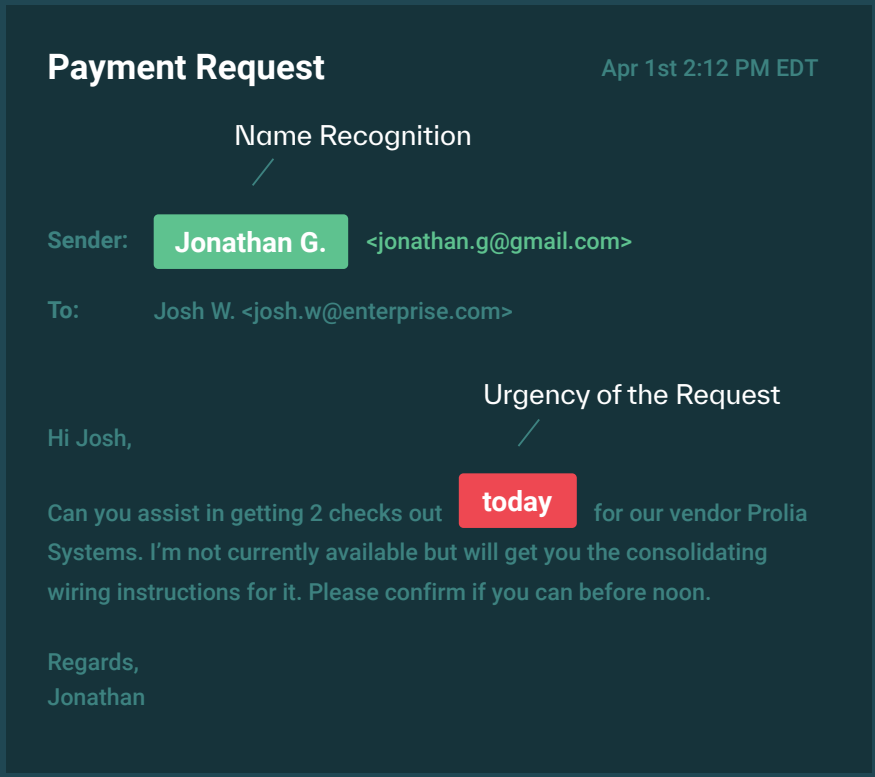
Secure email gateways look for known bad or indicators of compromise, like bad domain reputation, suspicious links, or malicious attachments. But since vendor compromise attacks do not make use of these tactics, they evade conventional defenses.

For many organizations, security awareness training is used to train employees to spot discrepancies so they can determine whether or not the email is fraudulent. However, with VEC attacks, the emails come from real accounts and contain legitimate business information, adding to the credibility of the request. As a result, employees find it difficult—if not impossible—to detect when a VEC attack is underway.



Additionally, real email accounts are sent from legitimate domains that are likely to pass email authentication protocols like DMARC. As a result, if they are compromised, the email attacks sent from the account will not be stopped by authentication defenses that look for misaligned DMARC configurations or domain spoofing.

If you look at a real-world example of an attack that bypassed the SEG, you can see why traditional defenses fail.



When these attacks land in inboxes, they rely on name recognition and ongoing correspondence to steal money. By encouraging their victims to act quickly, they successfully trick people into making mistakes. And based on the number of successful attacks, more people fall for it each year—despite an increase in security awareness training.

With hundreds of thousands of dollars at stake with each malicious email, like the $753,000 shown here, it's becoming increasingly obvious that these attacks must be stopped before they can trick your employees.

Suspicious Domain?

No. This email is using a real vendor account and will thus pass all authentication checks.

Malicious Links?

No. This is a text-based email with legitimate links.

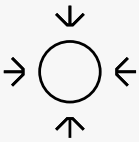
Corrupt Attachments?

No. This email has one attachment, but it is a benign file that looks exactly like other attachments sent from this account.

Abnormal SECURE|ANCHOR

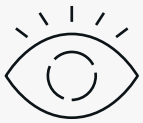
How to Stop Vendor Email Compromise Attacks

To counter these highly sophisticated attacks through trusted communications, organizations need the right technical controls to identify vendors that have been compromised. The next-generation type of email security includes:



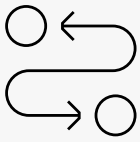
API Architecture

A solution that connects into Microsoft 365 and Google Workspace via an API and in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more.



Behavioral Data Science Approach

The solution should use a fundamentally different approach that leverages behavioral data science to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that include suspicious information or requests.



Federated Database of Vendor Behaviors

The solution should continuously monitor communications between vendors and customers, and provide a real-time assessment of vendor risk to inform decisions and stop targeted and sophisticated VEC attacks.

Without each of these capabilities, vendor email compromise will continue to outpace security measures—making it even more difficult to prevent these attacks from reaching employees, creating financial loss, and causing reputational damage.

Abnormal SECURE|ANCHOR

Abnormal

Conclusion

There is little doubt that vendor email compromise is a rising and financially damaging threat. By exploiting the trust organizations place in their vendors, these attacks dupe both humans and traditional email security tools that rely on threat intelligence. Stopping these attacks requires implementing a solution that can detect and interpret the thousands of signals available through an API, and then block the emails that come from compromised accounts. It's only by stopping these attacks from reaching inboxes that we can truly ensure that our organizations will stay protected.

Interested in Stopping Vendor Email Compromise?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@AbnormalSec →

/ Dr. Eric Cole

SECURE|ANCHOR

A world renowned cybersecurity expert with more than 30 years of network security experience, Dr. Eric Cole is a distinguished security researcher and keynote speaker who helps organizations curtail the risk of cyber threats.

He has worked with a variety of clients ranging from Fortune 50 companies, to top international banks, to the CIA, for which he was a professional hacker. While he started his career on the offense, he is now fully dedicated to understanding the adversary so he can provide cost-effective solutions that actually work.

As a pioneer in the area of cybersecurity, he has been inducted into the Infosec Hall of Fame, awarded the Cyber Wingman Award from the US Air Force, received multiple accommodations from the CIA, and was part of the commission on cybersecurity for President Obama. He has been the featured speaker at many security events and also has been interviewed by several chief media outlets such as CNN, CBS News, FOX News, and 60 Minutes.

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, vendor email compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Abnormal SECURE|ANCHOR

 v1.1/Mar. 2023