The Evolving Threat of Vendor Email Compromise and a Recent Incident Targeting an Alberta Organization

Executive Summary

On May 27th, 2025, an Alberta-based organization was targeted by a threat actor impersonating a trusted third-party vendor attempting to fraudulently redirect funds. This type of attack, known as Vendor Email Compromise (VEC), is similar to the more commonly known Business Email Compromise (BEC), but is distinguished by the specific impersonation of vendors known to the target organization. In this incident, a threat actor compromised a member of the target organization's mailbox, enabling monitoring of ongoing business communications. After identifying an ongoing invoice conversation, the threat actor hijacked the email thread, sending a PDF letter impersonating the vendor, requesting the fraudulent redirection of payment to a threat actor-controlled account.

This attack occurred shortly before researchers at Abnormal AI released a report demonstrating high levels of engagement with VEC attacks, driven by increasingly sophisticated levels of social engineering tactics. A similar incident targeting Ireland's National Treasury Management Agency (NTMA) successfully impersonated a known third-party investment company to steal €5 million Euros (~$8 million CAD). Taken together, these recent events in the province and beyond show that cyber threats are becoming more advanced. To stay safe, organizations should follow strict steps to verify transactions and encourage staff to question and report anything that seems unusual.

Vendor Email Compromise

VEC is the malicious act of impersonating legitimate third-party vendors to socially engineer unsuspecting victims into committing fraudulent payments to the threat actor. These attacks result from either a compromise of the target organizations mailbox, or the mailbox of the target organizations vendors. If a foothold in either email environment is achieved, the threat actor will perform deep reconnaissance on communications between the target and the vendor, enabling significantly more convincing lures.

After gaining an understanding of who the trusted vendors are, the threat actor can impersonate the vendors and assume the identity of their representatives. Domains that bear a likeness to the vendor will likely be created, using techniques such as typosquatting, use of an alternative top-level domain (TLD), or subdomain takeover. Most alarmingly, if vendors themselves have suffered a prior compromise, threat actors can then abuse their legitimate infrastructure for launching VEC attacks, helping bypass email security measures in place.

Example Company	Impersonation Method	Example Impersonation
`vendorname.ca`	Typosquatting	`accounts@vend0rname.ca`
	Alternative TLD	`accounts@vendorname.com`
	Subdomain Takeover	`abandoned-subdomain.vendorname.ca`

Table 1 - Examples of domain impersonations that could be leveraged in VEC attacks.

Other common techniques used by threat actors to increase the efficacy of their VEC attacks include:

- Hijacking email threads between the victim and the legitimate vendor, exploiting the existing trust and context to insert malicious instructions.
- Creating a false sense of urgency by claiming an invoice is overdue or requires payment, pressuring the target to act quickly without proper verification.
- Claiming the impersonated vendor's bank details have been changed, with the intent of redirecting payments to threat actor-controlled accounts.
- Stealing and modifying legitimate invoices from compromised mailboxes, using them as a template to create convincing fraudulent versions with the threat actor's banking information substituted in.

While these attacks require significant time and effort to plan and execute, the result is highly convincing and difficult to distinguish from routine business operations.

Recent Analysis by Abnormal AI

Between the period of March 2024 to March 2025, threat researchers at Abnormal AI monitored the mailboxes of over 1,400 client organizations. They tracked occurrences of what they refer to as "second-step engagement", a term used to describe when a user replies to a VEC email or forwards it to a non-phishing mailbox. The analysis revealed that the top three sectors with the highest levels of second-step engagement with VEC attacks were:

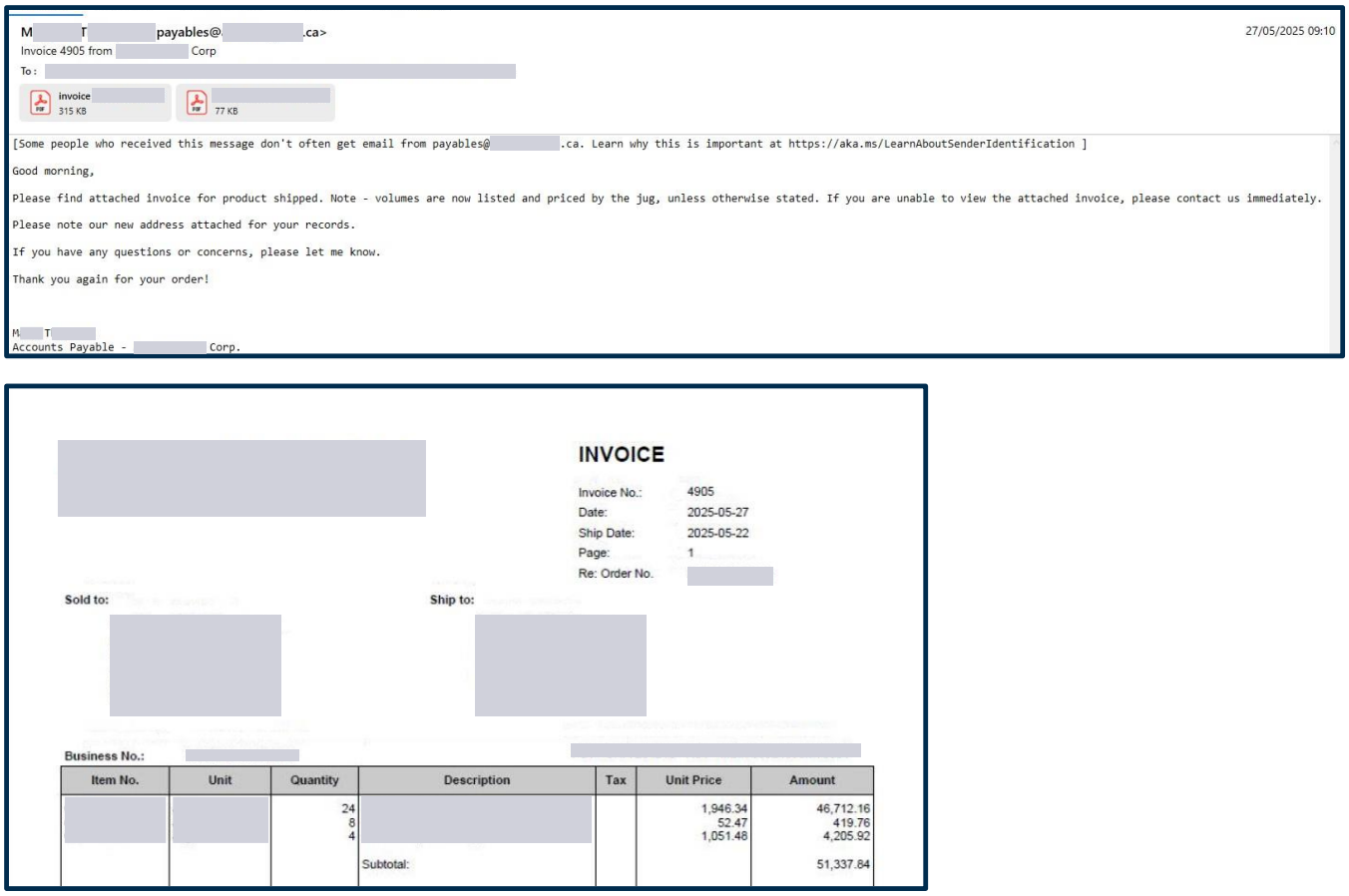
1. Telecommunications
2. Energy
3. Hospitality

High engagement was also observed across several other sectors, including critical infrastructure. Unsurprisingly, employees in accounting or sales roles showed the highest rates of engagement with VEC attacks, project managers also ranked among the most frequently engaged job categories.

Incident Affecting Alberta-based Organization

Recently, CyberAlberta was alerted to a VEC attack targeting an Alberta-based organization that was successfully detected, preventing any loss in funds. The threat actor had gained access to the organization's email environment and remained dormant to observe ongoing communications. After identifying an ongoing order with a local third-party vendor, the threat actor saw an opportunity to attempt a fraudulent redirection of the associated invoice payment.

Figure 1 below shows the last legitimate email and attached invoice, sent by the vendor representative (referred to here as M.T. to preserve anonymity), prior to the threat actor's attempt.



M T payables@ .ca>
27/05/2025 09:10
Invoice 4905 from Corp
To:
invoice 315 KB
77 KB

[Some people who received this message don't often get email from payables@ .ca. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification]

Good morning,

Please find attached invoice for product shipped. Note - volumes are now listed and priced by the jug, unless otherwise stated. If you are unable to view the attached invoice, please contact us immediately.

Please note our new address attached for your records.

If you have any questions or concerns, please let me know.

Thank you again for your order!

M T
Accounts Payable - Corp.

INVOICE

Invoice No.: 4905
Date: 2025-05-27
Ship Date: 2025-05-22
Page: 1
Re: Order No.

Sold to:

Ship to:

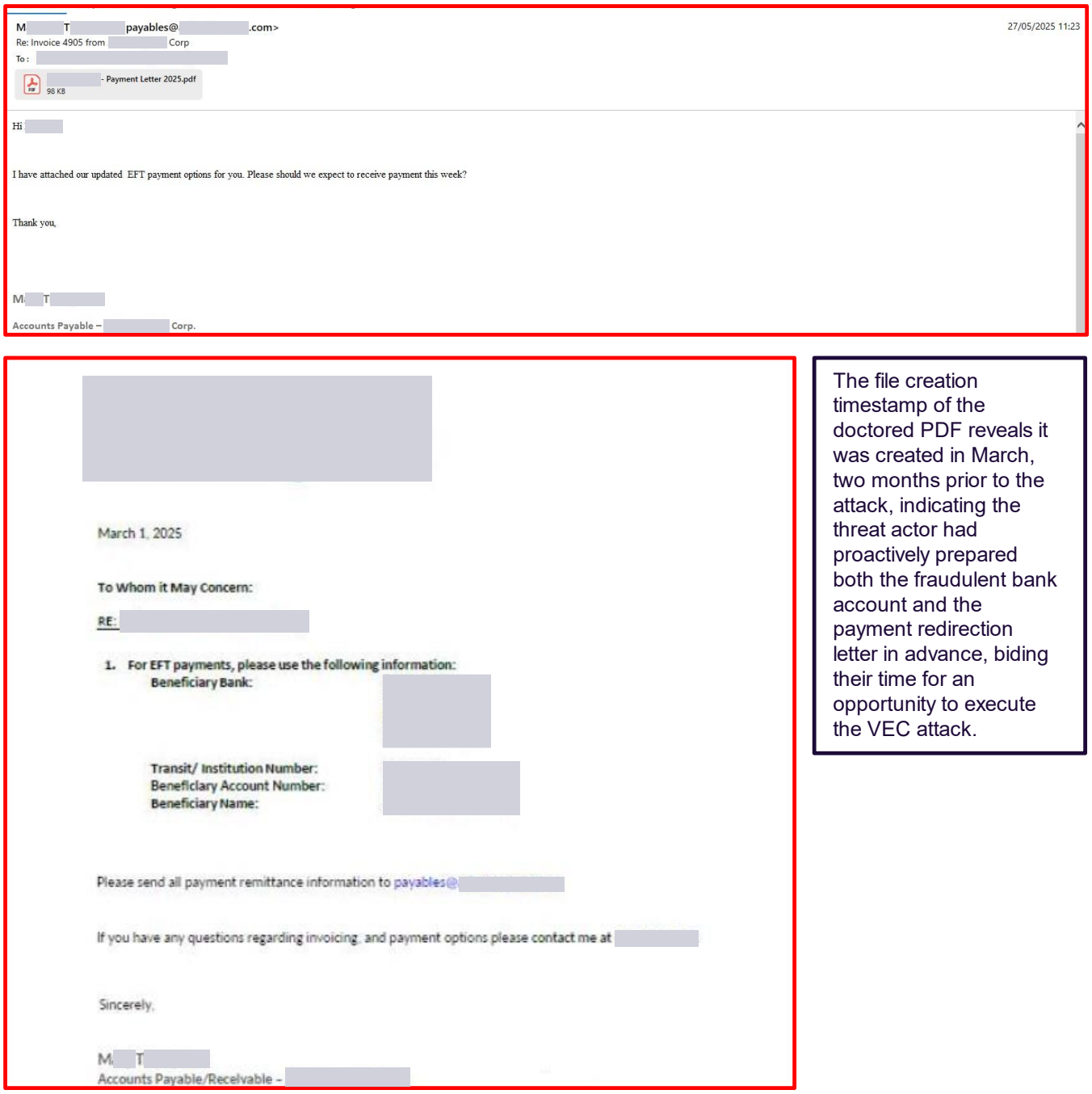
Business No.:

Item No.	Unit	Quantity	Description	Tax	Unit Price	Amount
		24			1,946.34	46,712.16
		8			52.47	419.76
		4			1,051.48	4,205.92
			Subtotal:			51,337.84

Figure 1 - Last email from the legitimate vendor representative prior to the attempted fraudulent payment redirection, notifying the organization of an invoice that is due payment.

The target organization responded to this legitimate email from the vendor, asking if they have an Electronic Fund Transfer (EFT) option available. At this point, the threat actor intervened—impersonating M.T.—and sent a forged email containing a doctored PDF that falsely claimed the vendor updated their bank details for EFT. To increase pressure, the threat actor also asked whether the payment could be processed within the same week.

The threat actor's malicious email and corresponding PDF letter can be seen below in Figure 2.



M T payables@ .com>
27/05/2025 11:23
Re: Invoice 4905 from Corp
To :
- Payment Letter 2025.pdf
98 KB

Hi

I have attached our updated EFT payment options for you. Please should we expect to receive payment this week?

Thank you,

M T
Accounts Payable – Corp.

March 1, 2025

To Whom it May Concern:

RE:

1. For EFT payments, please use the following information:
   Beneficiary Bank:

   Transit/ Institution Number:
   Beneficiary Account Number:
   Beneficiary Name:

Please send all payment remittance information to payables@

If you have any questions regarding invoicing, and payment options please contact me at

Sincerely,

M T
Accounts Payable/Receivable –

The file creation timestamp of the doctored PDF reveals it was created in March, two months prior to the attack, indicating the threat actor had proactively prepared both the fraudulent bank account and the payment redirection letter in advance, biding their time for an opportunity to execute the VEC attack.

Figure 2 - Malicious email and doctored PDF from the threat actor impersonating the vendor representative M.T., fraudulently claiming the vendor has changed the payment details to the threat actor controlled account.

Visually, the attack is highly convincing. The threat actor impersonates M.T., hijacks a legitimate email thread, retains the original subject line containing the known invoice number, and even replicates the vendor's logo in the doctored PDF. But what makes this—and similar attacks—particularly deceptive is that it occurs within the context of a legitimate, pre-scheduled payment, making it far less likely to raise suspicion.

To the average user, the only noticeable difference is the email sender domain.

- The vendor representative sent emails from a `.ca` domain address (payables@[vendor-domain].ca).
- The threat actor intervened with malicious emails from an impersonating `.com` domain address (payables@[impersonating-vendor-domain].com).

It was this subtle discrepancy, identified by a vigilant user, that exposed the attack and ultimately prevented the loss of over 50,000 CAD. However, the same threat actor was also linked to another VEC attack targeting other Alberta-based organizations which did result in a minor financial loss. This demonstrates how such attacks are rarely confined to a single target and will opportunistically pursue financial extortion wherever possible.

Recommendations

To help prevent VEC attacks, organizations are encouraged to implement the following measures:

- **Incorporate VEC Into User Awareness Training:** Reference this report when updating user awareness training materials. Ensure targeted training is provided to staff in accounting, sales, and project management roles, or any roles responsible for processing payments to third parties.
- **Enable Email Authentication Protocols:** While primarily applicable to vendors, it is best practice for all organizations to implement DMARC along with SPF and DKIM on their domains. These protocols help prevent threat actors from spoofing domains to deliver VEC attacks.
- **Strengthen Incident Response for VEC Attacks:** In an event of a detected VEC attack, network defenders should consider the following actions:
  - **Reset credentials** for any mailbox accounts suspected of compromise and ensure multi-factor authentication (MFA) is enabled across all users.
  - **Conduct threat hunting** for similar emails from the threat actor, using indicators such as the sender domain, sender display name, email subject, or attachment names to identify any other attempted VEC attacks.
  - **Audit mailbox rules** for suspicious forwarding or auto-delete rules that have been implemented by the threat actor to avoid detection.
  - **Review user account groups** for any anomalous account creations or modifications that grant access either to potentially compromised mailboxes, or other sensitive areas of the email environment.