Case Study

Account Update / Invoice Fraud Attack

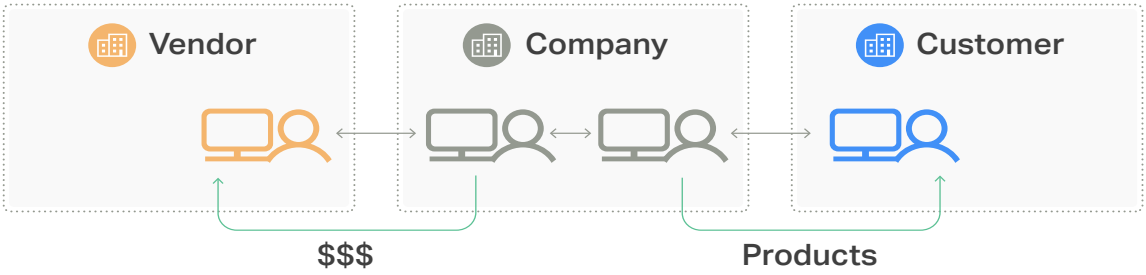
Overview

On April 8, 2020, Abnormal Security detected and stopped an attempted invoice fraud targeting a telecommunications provider, preventing more than $700,000 from being lost. The attacker's sophisticated operation lasted over 9 weeks. This case study details the sequence of events leading up to the actual attempt.

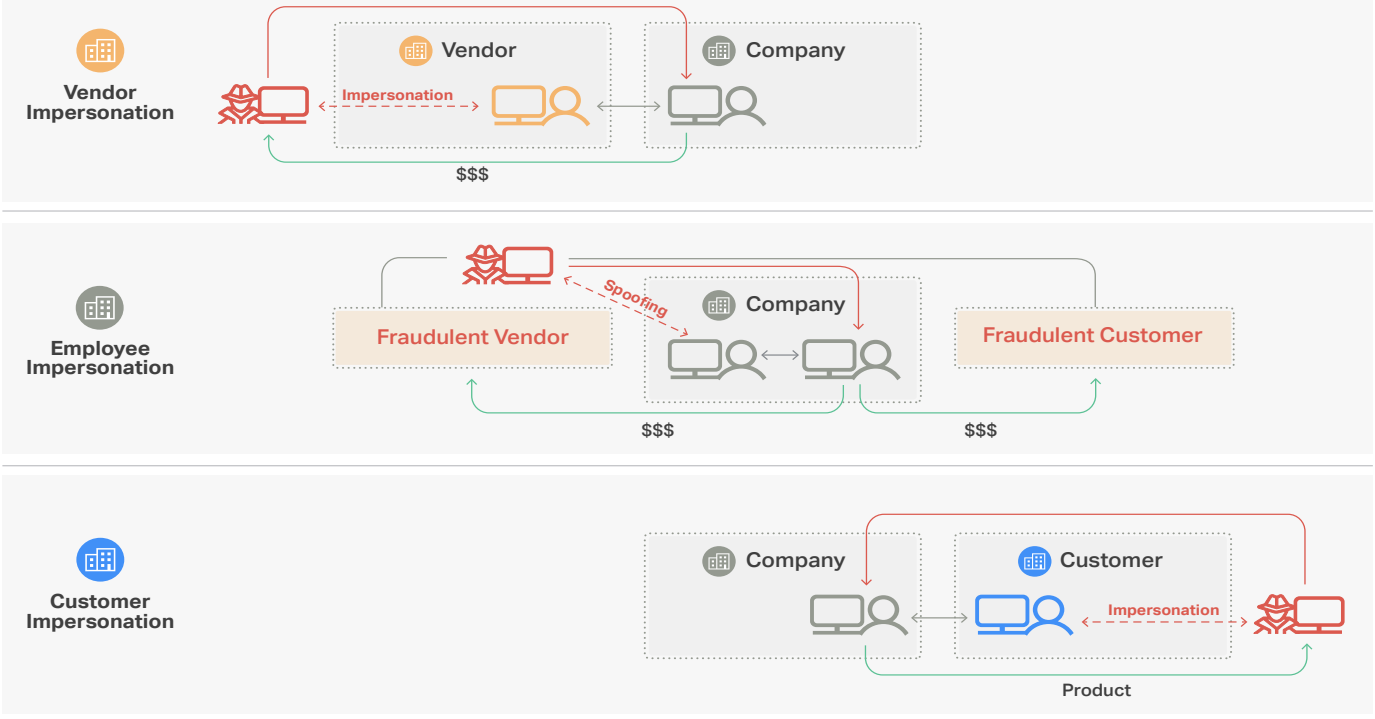
Disclaimer: All parties have been anonymized for this case study.

Types of Business Email Compromise (BEC) Attacks

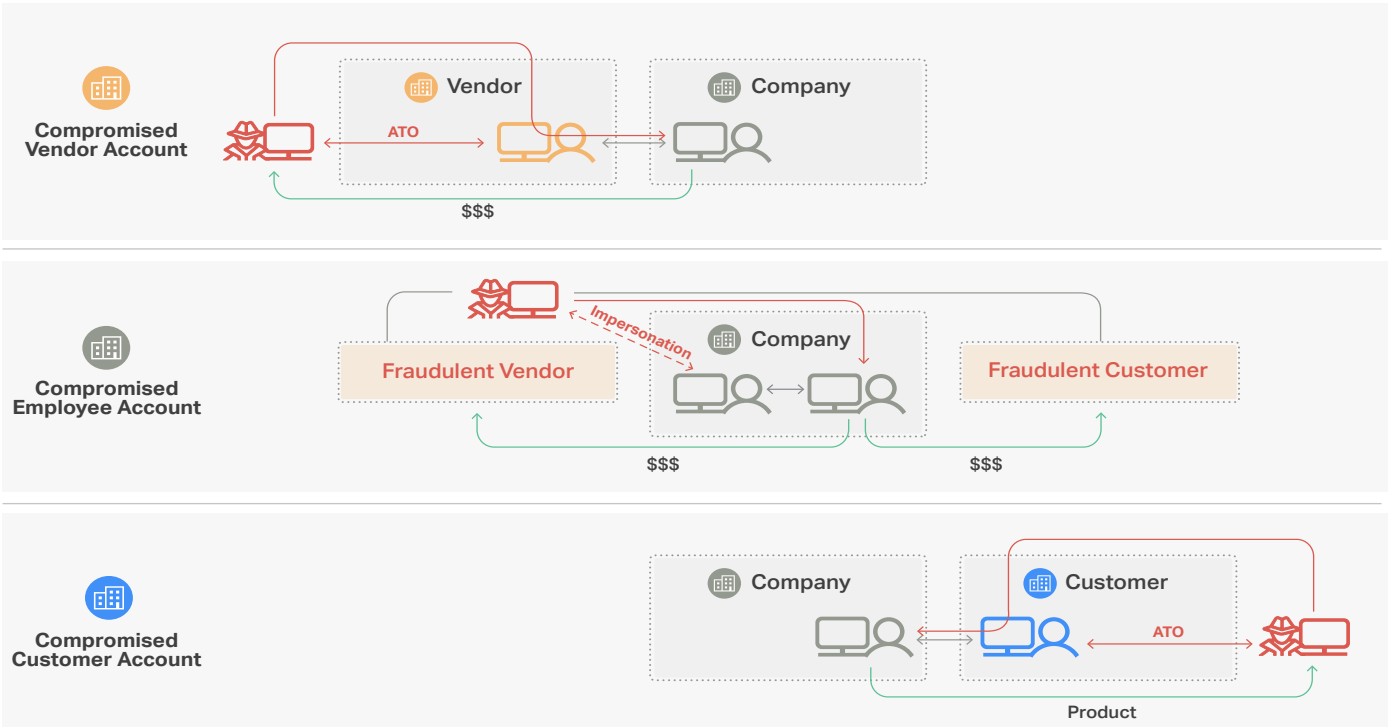
BEC attacks can be broken into 9 different categories depending on the pretext of the attacker (Vendor, Employee, Customer), along with the attack technique (Spoofing/Impersonation, or Compromised Account/Account Takeover). Attacks may also leverage a hybrid approach using multiple techniques.



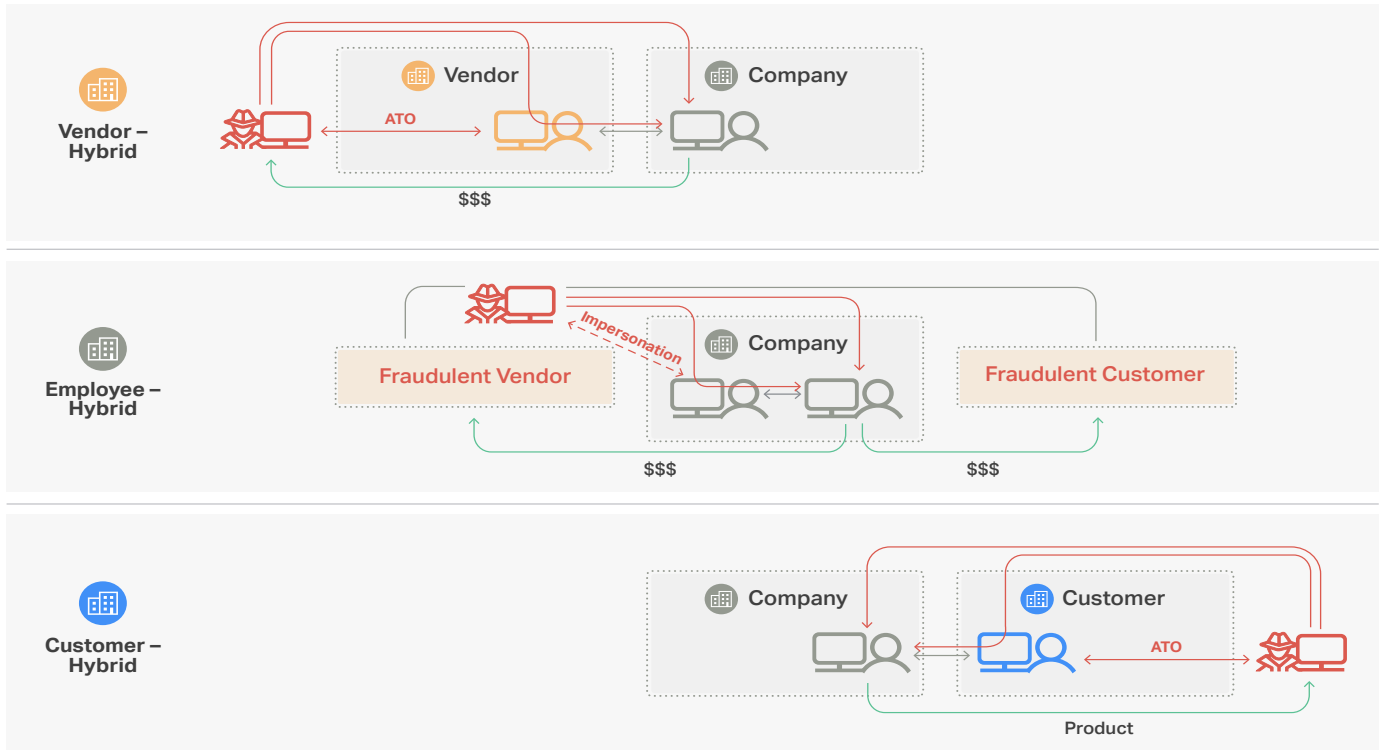
Impersonation (e.g., altered/lookalike domains)



Compromised Account (e.g., altered/lookalike domains)



Hybrid (e.g., altered/lookalike domains)



Attack Summary

The actor targets a telecommunications company (henceforth referred to as "TCC") by impersonating a vendor. The vendor is a real company, but is being impersonated by the attacker (henceforth referred to as "Impersonated-DC") using domain impersonation. Over the course of 2 months, the attacker convinces TCC to change banking details and redirect the payment of a legitimate invoice to the attacker's account. The amount of the invoice in question is worth over $700,000.

Constituents

Attacker Personas:
Impersonated Datacenter Provider (aka "I-DC")

- Clara Cooper (CFO)
- Amanda Steineman
- John Hickey
- Dylan Kessler
- Chris Force

Target Organization:
Telecommunications Company (aka "TCC")

- Megan: Accounts Payable
- Erin: Accounts Payable
- Ryan: Accounts Payable
- Paul: Accounts Payable
- Tina: Supply Chain Administrator

Attack Timeline

Attacker | **Target**

Attacker poses as CFO, emails from I-DC account notifying TCC of a change in banks and requests updated forms for EFT/ACH.

Feb 4, 2020

From: Carla Cooper
Sent: Tuesday, February 4, 2020 9:18 AM
To: Accounts Payable Help Desk
CC: Amanda Steineman, John Hickey, Dylan Kessler, Chris Force
Subject: ACH Information Update

Hello AP,

We are in the process of ending our relationship with our old bankers and the account will be closing Today.

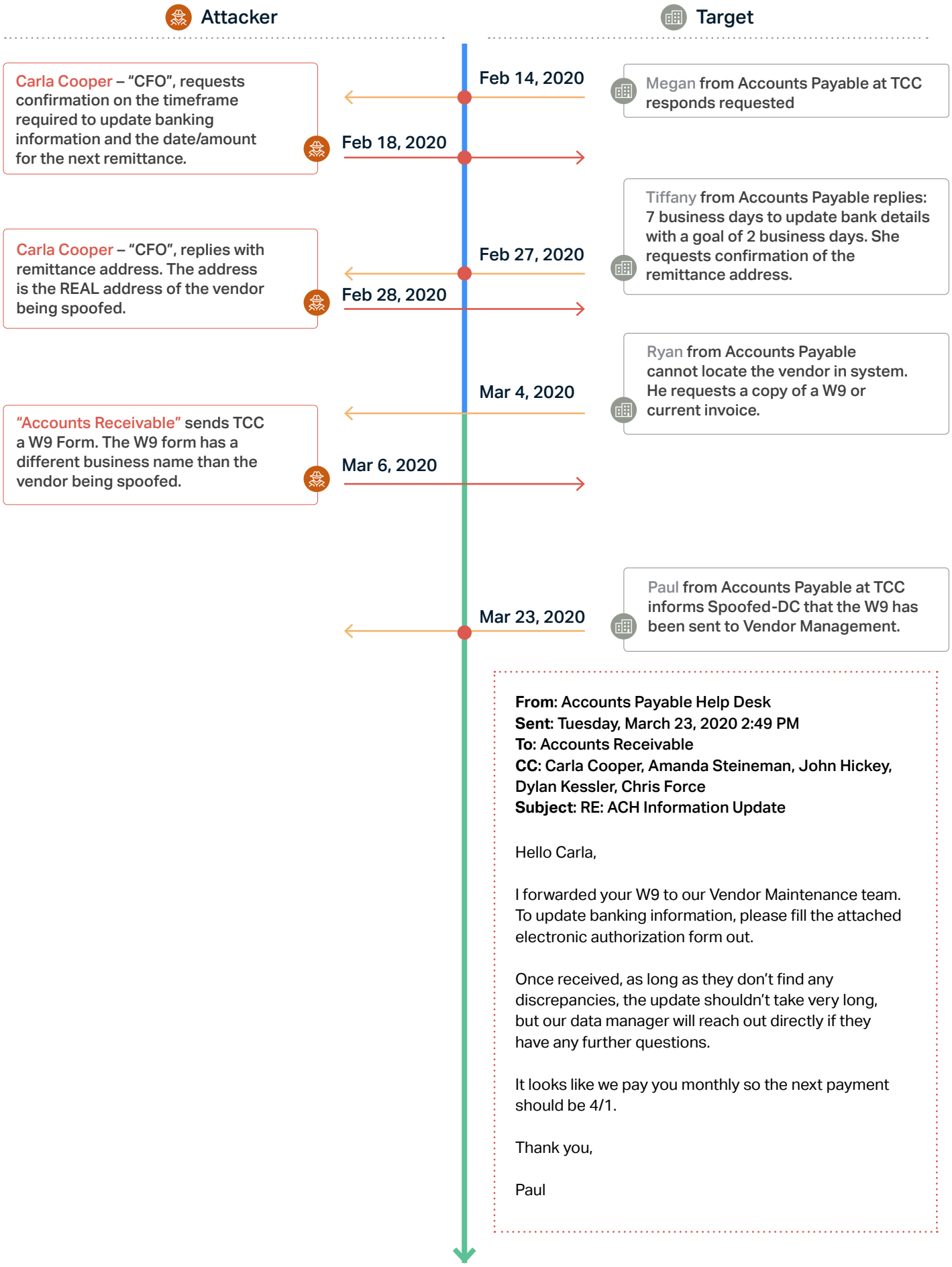
Could you please send me an update form for EFT/ACH transfers as I would like to uppdate our company bank details with you to receive all future payments.

However, Please cancel all EFT/ACH payments scheduled to our old account as it would not be received by us.

Your prompt response would be appreciated.

Thank you,

Carla Cooper
Chief Financial Officer
<Redacted> Network LLC


Attacker
Target
Carla Cooper – "CFO", requests confirmation on the timeframe required to update banking information and the date/amount for the next remittance.
Feb 14, 2020
Megan from Accounts Payable at TCC responds requested
Feb 18, 2020
Tiffany from Accounts Payable replies: 7 business days to update bank details with a goal of 2 business days. She requests confirmation of the remittance address.
Carla Cooper – "CFO", replies with remittance address. The address is the REAL address of the vendor being spoofed.
Feb 27, 2020
Feb 28, 2020
Ryan from Accounts Payable cannot locate the vendor in system. He requests a copy of a W9 or current invoice.
Mar 4, 2020
"Accounts Receivable" sends TCC a W9 Form. The W9 form has a different business name than the vendor being spoofed.
Mar 6, 2020
Paul from Accounts Payable at TCC informs Spoofed-DC that the W9 has been sent to Vendor Management.
Mar 23, 2020
From: Accounts Payable Help Desk
Sent: Tuesday, March 23, 2020 2:49 PM
To: Accounts Receivable
CC: Carla Cooper, Amanda Steineman, John Hickey, Dylan Kessler, Chris Force
Subject: RE: ACH Information Update
Hello Carla,
I forwarded your W9 to our Vendor Maintenance team. To update banking information, please fill the attached electronic authorization form out.
Once received, as long as they don't find any discrepancies, the update shouldn't take very long, but our data manager will reach out directly if they have any further questions.
It looks like we pay you monthly so the next payment should be 4/1.
Thank you,
Paul

Attacker Techniques

The actor behind this attack slowly engaged numerous employees over the course of two months, and leveraged both simple and sophisticated techniques to execute and progress this attack. Highlights of key techniques are enumerated below.

Domain Impersonation

The attack was an impersonated vendor. Common techniques for domain impersonation include:

- Replacing "***i***" with "***l***"
  e.g., "redbird.com" becomes "redblrd.com"
- Adding an "***s***"
  e.g., "advancednetwork.com becomes "advancednetworks.com"
- Adding "***int***" or "***inc***"
  e.g., "superiorpackaging.com" becomes "superiorpackaginginc.com"

Adding multiple personas from the Impersonated Vendor

To add greater credibility to the initial email for engagement, the actor included five (5) additional (impersonated employees from the impersonated vendor), presumably accounts receivable or other G&A employees.

Initial request is very low risk

The initial outreach from the actor makes a very low risk and low consequence request. The attacker ("Carla Cooper") is simply asking for an EFT/ACH transfer form. No sensitive information has been sent or communicated at this point. However, once the initial engagement has occurred, an email chain is established and subsequent interactions with other employees are met with less and less suspicion as the engagement continues to deepen.

Detection Techniques

Abnormal Security detected this attack and prevented the payment to the incorrect account from occurring. This attack was detected during an evaluation of the product in passive mode, enabling a unique view of the entire lifecycle of the attack. The core of Abnormal Security's detection is Abnormal Behavior Technology, or ABX, which combines the Abnormal Identity Model, Abnormal Relationship Graph, and Abnormal Content Analysis to arrive at high confidence decisions. A number of specific techniques in ABX were used to detect this attack, including:

Identity Modeling

VendorBase: A global, federated database on vendor to provide real-time scores of vendor risk.

Domain Impersonation: Identification of a lookalike domain raised suspicion of a potential attack.

Relationship Graph

Normalcy Traits: Geolocation and key contacts at each vendor

Domain Analysis: Pattern and age of domain

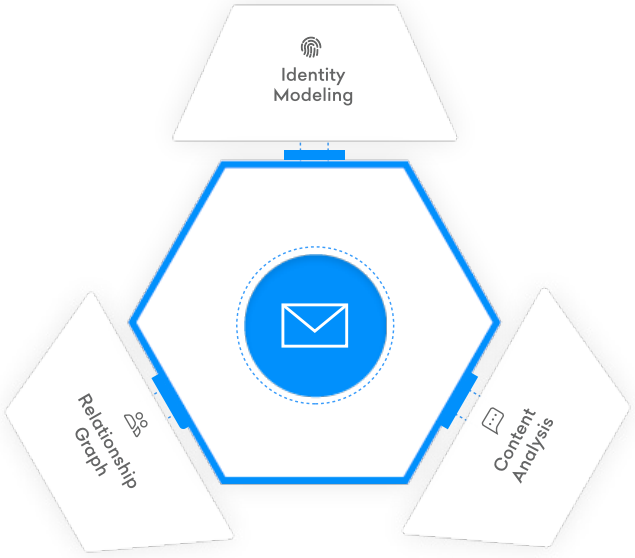
Unsafe engagements: Unusual and unsafe engagement from employees

Content Analysis

Natural Language Processing: Text analysis to determine topic and sentiment of conversation.

Vendor Mail Detector: Model to automatically detect vendor relationships.

Invoice Processing: Detection of invoices for invoice-specific analysis.



For more information about how Abnormal Security detected this and many other types of attacks, please visit: www.abnormalsecurity.com

About Abnormal Security

The Abnormal Security cloud email security platform protects enterprises from targeted email attacks. Powered by Abnormal Behavior Technology (ABX), the platform combines the Abnormal Identity Model, the Abnormal Relationship Graph and Abnormal Content Analysis to stop attacks that lead to account takeover, financial damage and organizational mistrust. Through one-click, API-based Office 365 and G Suite integration, Abnormal Security sets up in minutes, requires no configuration and does not impact email flow. Backed by Greylock Partners, Abnormal Security is based in San Francisco, CA. Please visit www.abnormalsecurity.com and follow the company at @AbnormalSec.

Contact Us

www.abnormalsecurity.com

@AbnormalSec

797 Bryant Street
San Francisco, California 94107