Abnormal Security

White Paper

ABX: Abnormal Behavior Technology

Executive Summary

Business email compromise (BEC) was recently described by Fortune magazine as "one of tech's most pernicious threats." The FBI's Internet Crime Complaint Center (IC3) reports that financial losses from BEC attacks have doubled year over year since 2016 and currently represent nearly 50% of all financial losses in cybersecurity.[1] A report from AIG recently highlighted BEC as the number one reason for cyber-insurance claims[2] – exceeding ransomware. Many organizations have also reported that the FBI has been unable to assist with cases of financial loss less than $1M. This lower limit has grown over the years due to case workload.

Email has been the leading attack vector for cyberattacks for years. Security organizations have responded by investing heavily in email security solutions to combat everything from commodity spam to ransomware in attachments to credential phishing. And yet, BEC losses continue to grow in spite of this awareness.

The FBI's Internet Crime Complaint Center (IC3) reports that financial losses from BEC attacks have doubled year over year since 2016 and currently represent nearly 50% of all financial losses in cybersecurity.[1]

To evade detection from current email security solutions, increasingly sophisticated attacks rely on social engineering and do not contain malicious payloads. Emails are delivered from reliable domains (e.g. gmail.com) or via newly created infrastructure thanks to the ease offered by cloud services, and thus bypass detection by reputation.

Clearly, a new approach is needed to defend enterprises and to reclaim confidence and trust in email, the most critical business communication medium.

Abnormal Behavior Technology (ABX) leverages patent-pending techniques to provide a revolutionary approach to detecting targeted email attacks. The foundation of ABX is rooted in decades of experience in advertising technology that focused on understanding user behaviors with large-scale data science platforms. This unique, data science-based approach allows ABX to arrive at high-confidence detection of the toughest socially engineered email attacks. ABX learns from each customer environment, uniquely leveraging the broadest set of organization-specific data among all email security solutions to protect your enterprise.

Unlike other email security solutions, there is no need for customers to perform any tuning to deliver or maintain this high degree of effectiveness. Furthermore, by leveraging an API-based integration, deployment is fast and simple.

[1] https://pdf.ic3.gov/2016_IC3Report.pdf
https://pdf.ic3.gov/2017_IC3Report.pdf
https://pdf.ic3.gov/2018_IC3Report.pdf

[2] https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf

ABX: Abnormal Behavior Technology

What's the Problem with Email Security?

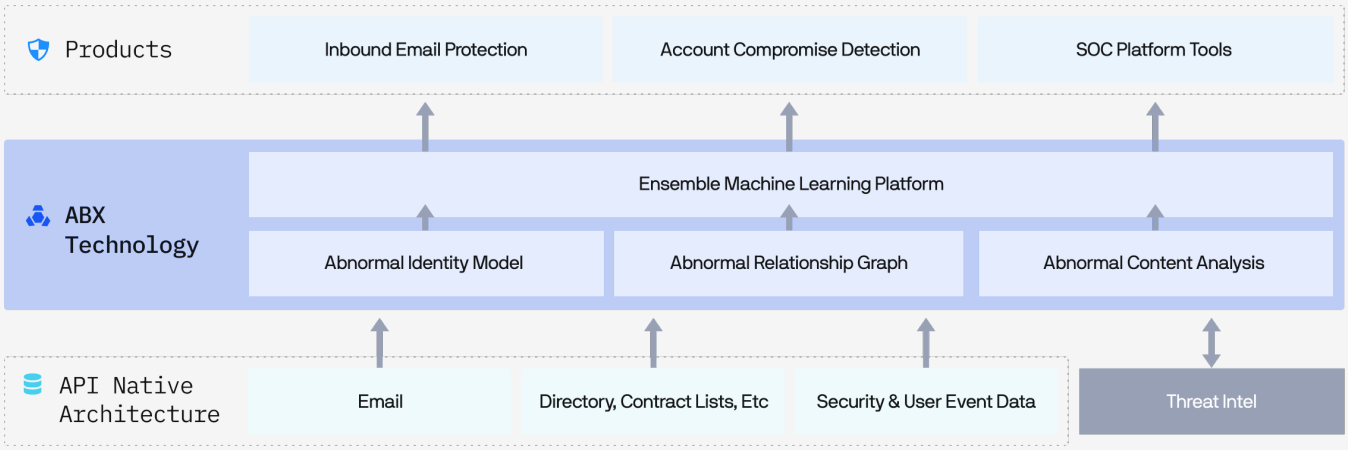
Socially engineered attacks such as BEC evade traditional email security solutions because they lack the common threat signals to trigger a detection. These attacks do not have attachments carrying malware. Nor do they contain URLs leading to malicious websites. The content of the email is generally simple, and the attacks are customized for each individual target.

BEC attacks, by nature, represent a small portion of the total email attack vector: these attacks are nearly always hand-crafted and incorporate heavy elements of social engineering, and thus their fraction of all email threats is resultingly tiny. As such, email security vendors who miss these attacks can still maintain claims of high efficacy rates due to the sheer volume of unwanted emails such as spam and malware campaigns that they stop. However, while a small percentage by comparison, BEC disproportionately represents the greatest financial risk.

The foundation of ABX is rooted in decades of experience in advertising technology that was focused on understanding user behaviors with large scale data-science platforms.

The Attack Framework

Abnormal Security has developed the following framework to break down the different types of socially-engineered email attacks.



ABX: Abnormal Behavior Technology

Examples of Emails that Bypass Traditional Solutions

01

Executive Impersonation

PRETEXT
Internal Employee (Executive)

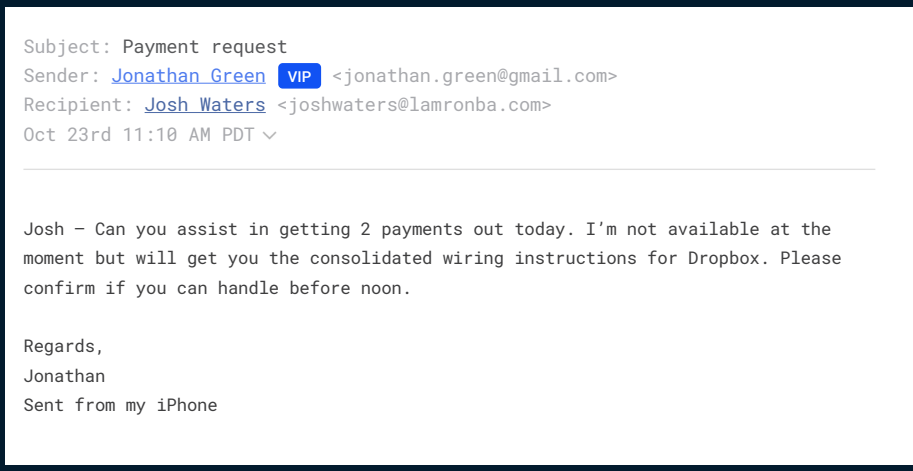
APPROACH
Impersonation

DELIVERY
No Payload

Executive Impersonation is a common example of BEC and one of the easiest for attackers to execute. These attacks are very challenging to detect due their simplicity and frankly, their elegance.

Emails may be coming from reliable and known email services such as Gmail. Due to the widespread use and general business need to communicate to individuals using these services, emails from those sending domains cannot be simply blocked.

Some enterprises implement rules for each executive by providing specific allowances for personal email addresses, but this is neither a foolproof nor a scalable solution.



Subject: Payment request
Sender: Jonathan Green VIP <jonathan.green@gmail.com>
Recipient: Josh Waters <joshwaters@lamronba.com>
Oct 23rd 11:10 AM PDT

Josh – Can you assist in getting 2 payments out today. I'm not available at the moment but will get you the consolidated wiring instructions for Dropbox. Please confirm if you can handle before noon.

Regards,
Jonathan
Sent from my iPhone

02

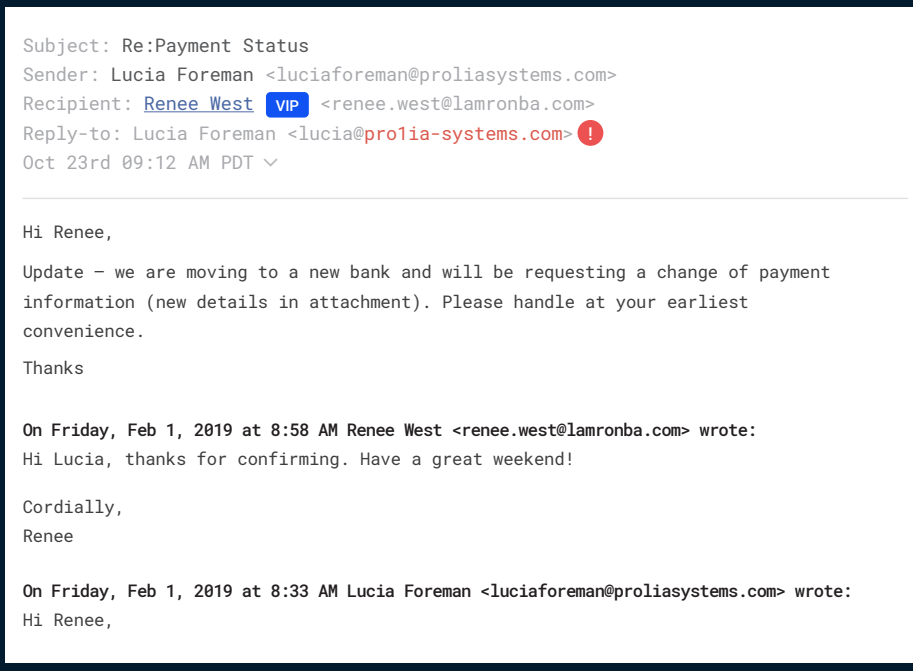
Vendor Compromise/ Conversation Hijacking

PRETEXT
External Partner (Vendor)

APPROACH
Compromised Account

DELIVERY
No Payload or Fake Invoice

Compromised vendor accounts are an extremely difficult attack to identify. The emails are coming from trusted relationships and attackers may reply back to an existing email thread to further seem credible.



Subject: Re:Payment Status
Sender: Lucia Foreman <luciaforeman@proliasystems.com>
Recipient: Renee West VIP <renee.west@lamronba.com>
Reply-to: Lucia Foreman <lucia@pro1ia-systems.com> !
Oct 23rd 09:12 AM PDT

Hi Renee,

Update – we are moving to a new bank and will be requesting a change of payment information (new details in attachment). Please handle at your earliest convenience.

Thanks

On Friday, Feb 1, 2019 at 8:58 AM Renee West <renee.west@lamronba.com> wrote:
Hi Lucia, thanks for confirming. Have a great weekend!

Cordially,
Renee

On Friday, Feb 1, 2019 at 8:33 AM Lucia Foreman <luciaforeman@proliasystems.com> wrote:
Hi Renee,

03

Employee Compromise

PRETEXT
Internal Employee

APPROACH
Compromised Account

DELIVERY
No Payload or Fake Invoice

Similar to compromised vendor accounts, attacks from internally compromised accounts are also extremely difficult to identify. Not only are the emails coming from trusted employees, the internal-to-internal (i.e., intra-domain mail flow) is not commonly scanned by traditional email security solutions.

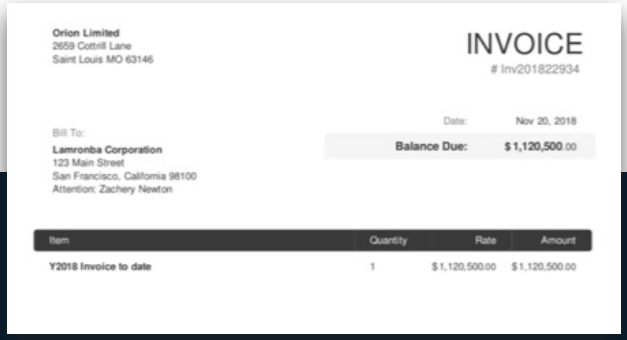
Subject: Orion Limited Invoice
Sender: Renee West VIP <reneewest@lamronba.com>
Recipient: Josh Waters <joshwaters@lamronba.com>
Oct 23rd 02:46 PM PDT

Zachary and Josh,

Please review the attached – I have approved this wire transfer and it should be prepared for immediate release.

Thanks,

Renee West
Treasurer
www.lamronba.com



04

Credential Phishing

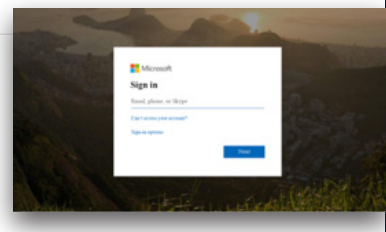
PRETEXT
Brand

APPROACH
Impersonation

DELIVERY
URL to a credential phishing site

Most credential phishing attempts are impersonation attempts of a known brand such as Microsoft, Amazon, FedEx, Google, etc. While some email security solutions may detect these attacks (high entropy URLs, previously seen URLs as part of a threat intelligence source, etc.) these attacks are difficult to reliably catch. The credential phishing sites do not typically contain malware making typical sandboxing approaches ineffective.

Subject: Office365 password expiry notice!!!
Sender: Acme Microsoft Support <asmith@acme.com>
Recipient: Adam Smith <ASmith@acme.com>
Nov 24th 05:30 PM PST



Password expiry notice!!!

User name: asmith@acme.com

Here's what to do next:

- Click the link below.
- Use the button below to re-confirm and continue with the same password.

Re-activate Password

If this issue isn't resolved, your subscription and any data you may have stored in it will be permanently deleted on 31 November 2019.

Sincerely,
The Acme Microsoft Support Team

Looking Beyond the Email

In the wake of successful BEC attacks, investigations from security teams expand beyond the scope of just the email. Examples of investigative activities stemming from a successful BEC attack include:

- CIRT teams look to identify the sender and whom they were impersonating
- Contacting an executive to verify personal email accounts in order to confirm an executive impersonation
- Contacting an impersonated vendor to verify bank account information (if the attacker had posed as a vendor and changed account information)
- Reviewing logs of internal accounts for evidence of a compromised account.

Oddly, none of the current email security solutions perform these activities while attempting to identify and block a socially engineered, targeted email attack.

ABX learns from each customer environment, uniquely leveraging the broadest set of organization-specific data among all email security solutions to protect your enterprise.

Abnormal Behavior Technology (ABX)

Abnormal Behavior Technology, or ABX, looks beyond email data and redefines the scope of behavioral analysis. ABX takes a data science approach, analyzing dozens of data sources specific to each organization to arrive at high-confidence decisions to block targeted email attacks.

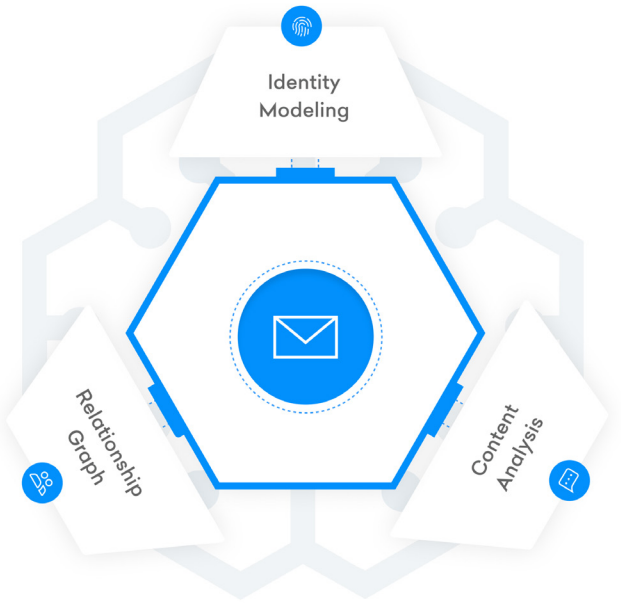
The roots of ABX derive from experience within the advertising technology space, where data scientists honed their craft analyzing user behaviors. With data beyond just email available via email platform APIs from Microsoft Office 365 and Google G Suite, organization-specific inputs can now be leveraged to identify email attacks.

ABX analyzes the rich data from dozens of data sources to profile communications across three distinct perspectives:

Abnormal Identity Model

Abnormal Relationship Graph

Abnormal Content Analysis



The results of the analysis across these three areas is then consolidated by an ensemble of machine learning algorithms to ensure a high-confidence verdict, minimizing false positives that plague traditional machine learning algorithms.

01

Abnormal Identity Model

The Abnormal Identity Model is a stateful model of both internal and external identities.

For employees, ABX takes inputs from the directory, analyzes user events, and analyzes email communications resulting in models for each employee. The attributes for each internal identity include:

Employee Identity Model

Name	Office Address
Email	Phone Number
Role	Term at Company
Personal Email	Browsers Used
Location	Devices Used
Sign-In Locations	Usual Login Time
Manager	Mail Filter Configuration
Manager Location	Client Applications Used
Department	Mailing Address
VIP Status	

ABX incorporates more sources of data than any other email security solution today.

External entities are modeled by evaluating the email communications in detail to extract identity attributes.

Vendor Identity Model

Vendor Name	Invoicing Software
Emails Used for Communication	Invoicing Cadence
Key Vendor Contacts	Communication Cadence
Key Internal Contacts	Bank Information / Accounts
Mailing Address	Invoicing Language
Verified email FQDN	Last Contacted
Phone	Years of Relationship

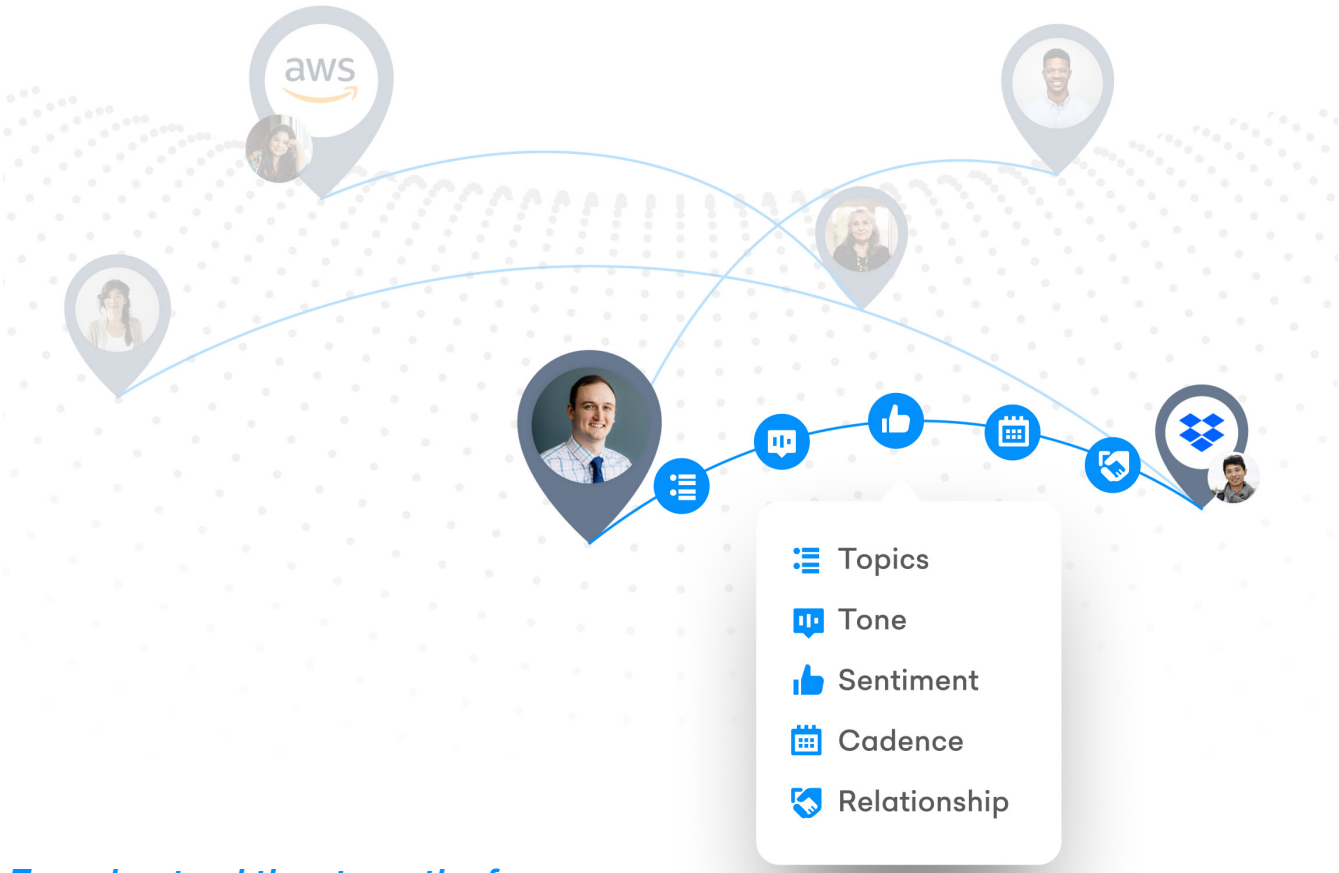
Customer Identity Model

Customer Name	Phone
Customer Emails	Invoice Frequency
Key Customer Contacts	Last Contacted
Key Internal Contacts	Years of Relationship
Mail Address	Communication Cadence
Verified Email FQDN	

02

Abnormal Relationship Graph

ABX profiles the communication patterns between individuals, departments and organizations to create the Abnormal Relationship Graph, which is continually updated. The Abnormal Relationship Graph provides an understanding of the strength of each connection by analyzing the frequency of communication along with the topic and tone of each email. Unusual communications can be identified from rare or never-before-seen paths. Or normal communication paths may have abnormal topics and sentiment.



To understand the strength of each connection, the frequency of communication is analyzed along with the topic and tone of each email communication.

03

Abnormal Content Analysis

Email content is analyzed by ABX using a variety of techniques, including:

Deep URL Analysis

Link chains are followed to the final destination to ensure a complete and thorough analysis of what an end-user would be exposed to. URLs contained within attachments are also analyzed.

Computer Vision Techniques

Computer vision algorithms analyze URL landing pages to identify brands and form layouts. Attachments are also analyzed using these techniques to identify logos as well as extract information contained within the document.

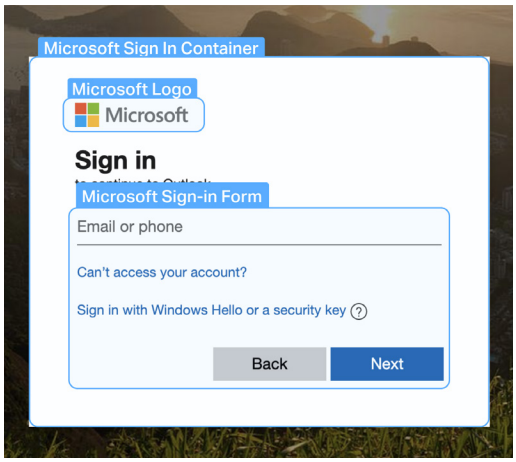


Figure 1: Computer vision algorithms analyze URL landing pages

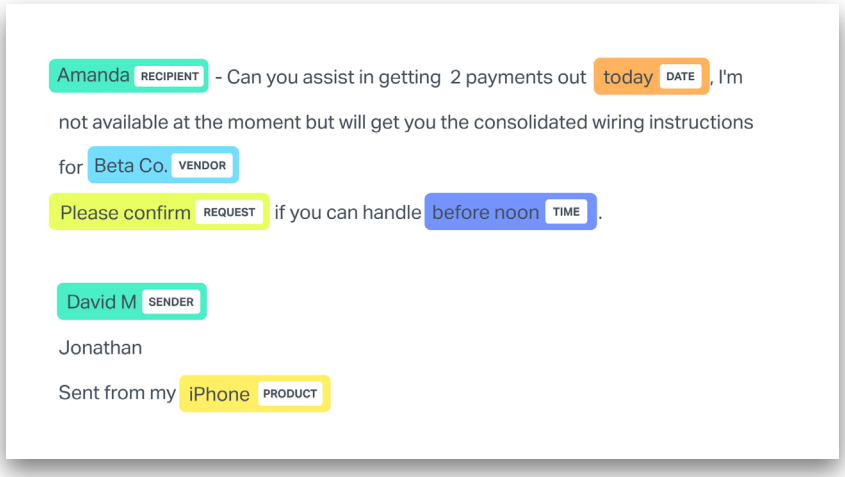


Figure 2: Natural Language Processing (NLP) algorithms identify Topic, Tone and Sentiment

Natural Language Processing

Natural Language Processing (NLP) algorithms identify Topic, Tone and Sentiment within communications. BEC attacks typically feature urgent requests on financial topics, so identifying these types of communications can assist in the accurate detection of attacks. NLP algorithms are also used to help establish the Abnormal Relationship Graph by understanding the types of communication (e.g., formal vs. informal) that are occurring between individuals, departments and organizations.

Threat Intelligence

ABX leverages threat intelligence feeds to block known bad signals such as URLs/domains.

04

Composite Analysis: Ensemble Machine Learning Algorithms

An ensemble of machine learning algorithms evaluates the signals generated by the trio of perspectives from the Abnormal Identity Model, the Abnormal Relationship Graph, and the Abnormal Content Analysis. The algorithms identify specific types of attacks and techniques and result in a final email disposition that is delivered along with clear, concise, and explainable insights for the human analyst to review.

Explainable Insights

Most solutions that leverage machine learning technologies result in "black-box" outputs. Some results make sense. Others may not, but users have no mechanism of understanding why and how the algorithms reached a specific conclusion.

Abnormal's decision engine explains and summarizes the automated analysis of thousands of signals that were used to detect the attack.

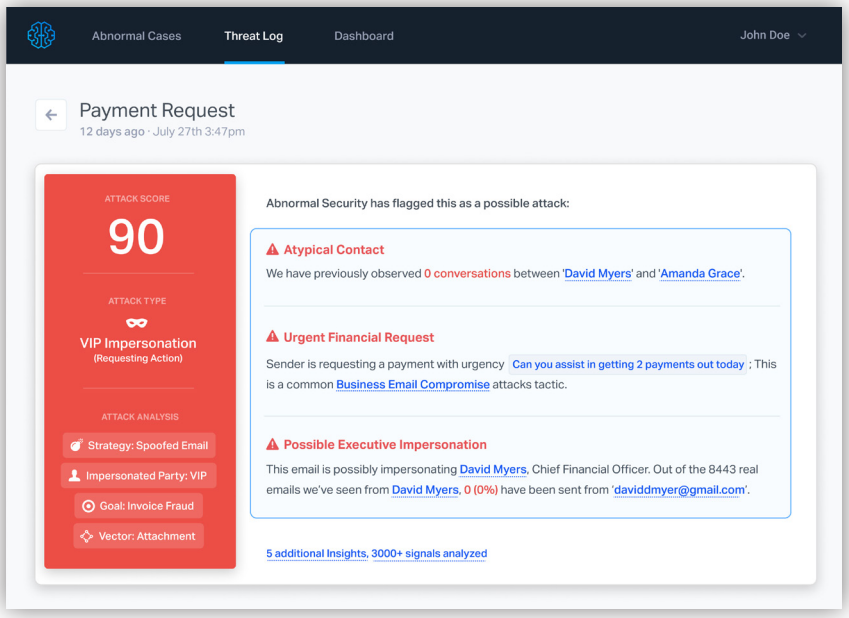


Figure 3: Automated analysis and attack classification in a single view provide a clear overview to assist in next steps

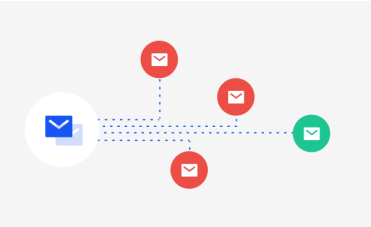
ABX: Abnormal Behavior Technology

The Abnormal Email Security Platform

Powered by ABX, the Abnormal Email Security Platform protects organizations with a cloud-native email security platform designed to augment Microsoft Office 365 and Google G Suite. The native security capabilities of Office 365 and G Suite handle the widespread threats, including broad spam and phishing campaigns, while Abnormal Security uses its unique behavioral approach to address the sophisticated, targeted attacks.

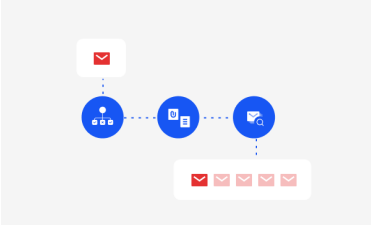
The Abnormal Email Security Platform provides 3 core capabilities:

Powered by ABX, the Abnormal Email Security Platform protects organizations with a cloud-native email security platform designed to augment Microsoft Office 365 and Google G Suite.



1. **Inbound Email Protection**: stops the full range of email attacks, with a unique focus on modern social engineering attacks

2. **Email Account Compromise Detection**: looks beyond email and analyzes hundreds of signals to accurately detect compromised accounts



3. **SOC Platform for Email Response:** assists security operations teams with automation and tools to respond quickly to email threats

Integrating via API provides access to a broad set of data to enable ABX to analyze behaviors as well as monitor intra-domain email traffic (i.e., internal-to-internal) which traditional email security solutions are blind to. Additionally, the API-based architecture provides ease of integration and maintenance, with no MX record or mail routing changes required.

Conclusion

Abnormal Behavior Technology (ABX) uses a unique, data science-based approach to drive high-confidence detection of the toughest socially engineered email attacks such as BEC. ABX learns from each customer environment, uniquely leveraging a broad set of organization-specific data to protect your enterprise.

Abnormal Behavior Technology:

- Looks beyond email data
- Combines the Identity Model, Relationship Graph, and Content Analysis to drive accurate detection of email attacks
- Continuously self-tunes and adapts

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. Though 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.

Abnormal Security Corporation
797 Bryant Street
San Francisco, California 94107