2023 Email Security Threat Report
# Table of Contents

1. Executive Summary
2. Key Insights
3. Vendor Compromise Attacks Rising for Small and Medium Sized Technology Organizations
4. Business Workflows Involving User Data are Most Compromised
5. Language Remains Main Attack Vector to get BEC Attacks in Front of Employees
6. Financial Industry at the Receiving End of Financial Fraud Attacks
7. Malicious Actors Are Still Playing “Go Phish” with Legacy Solutions
8. Lifting the Mask on Impersonation Attacks
9. Smaller Organizations Are More Likely to Be Targets of Compromise Attacks
10. Security Teams Waste up to 27 Hours a Week Managing Graymail Manually
Executive Summary

We are pleased to present our second annual Email Security Threat Report, highlighting trends and changes in the threat landscape that Armorblox has observed across our broad customer base.

Over the past year, we have seen a significant shift in the types of attacks launched and the methods used by attackers. Unfortunately, native email security and inline security tools used to detect and prevent these attacks have proven insufficient.

As the threat landscape evolves, IT and security leaders must stay informed and take proactive measures to secure their organizations against cyberattacks. This report provides valuable information and insights to help organizations stay ahead of the curve and ensure data safety for themselves, their end users, and their clients.

Here at Armorblox, we protect over 58,000 organizations globally from targeted email attacks. We analyze over 4 billion emails and stop over 800,000 threats every month.

Here at Armorblox, we protect over 58,000 organizations globally from targeted email attacks. We analyze over 4 billion emails and stop over 800,000 threats every month. For this report, our threat research team compared threat data from 2022 to data collected from 2021’s report. The accompanying sections take a deep dive into the most prevalent threat types to present the current state of email security threats.
Key Insights

Vendor Compromise
Attacks Rising for Small and Medium-Sized Technology Organizations

Business Workflows
Involving User Data are Most Compromised

Language Remains Main Attack Vector to get BEC
Attacks in Front of Employees

Financial Industry at the Receiving End of Financial Fraud Attacks

Malicious Actors Are Still Playing “Go Phish” with Legacy Solutions

Lifting the Mask on Impersonation Attacks

Smaller Organizations Are More Likely to Be Targets of Compromise Attacks

Security Teams Waste up to 27 Hours a Week Managing Graymail Manually

Key Insights

56% of all attacks bypassed legacy security filters

Of all attacks seen across 2022, half bypassed legacy security filters (56%).

53% of vendor compromise attacks targeted technology organizations

Small and medium-sized businesses (SMBs) are particularly vulnerable to vendor fraud and supply chain email attacks. More than half of vendor compromise attacks targeted technology organizations (53%).

52% of all attacks involve sensitive user data

Bad actors are still infiltrating legitimate business workflows to steal sensitive business information. Half of all attacks involve sensitive user data, such as user login credentials (52%).

77% of BEC attacks that bypass legacy security involve language as the main attack vector

BEC attacks continue to evolve. Language remains the main attack vector in 4 out of 5 (77%) BEC attacks that bypassed legacy solutions in 2022.

58% of account compromise attacks targeted SMBs

With the widespread use of email for business communications, half of account compromise attacks targeted SMBs (58%), proving to be a persistent and prevalent threat.

27 hours per week are wasted on manual remediation of graymail by security teams

Security teams can find themselves spending upwards of 27 person hours a week manually sorting and deleting graymail across user mailboxes.
Vendor Compromise Attacks Rising for Small and Medium Sized Technology Organizations

Vendor fraud and supply chain attacks are becoming a concern for organizations of all sizes. These attacks exploit the trust between organizations and their suppliers, and can result in significant financial losses or reputational damage. The Armorblox Research Team looked at this year’s trends and data on vendor fraud and supply chain attacks to provide insights for organizations looking to protect themselves against these threats.

In 2022, organizations within the Technology Industry had the highest chance (53%) of being the target of a vendor compromise attack.

Vendor Compromise Attacks by Industry

- **Technology**: 53%
- **Financial**: 10%
- **Software**: 8%
- **Other**: 29%
Vendor Compromise Attacks Rising for Small and Medium Sized Technology Organizations

Small and medium-sized businesses are particularly vulnerable to vendor fraud and supply chain email attacks. Armorbox data suggests bad actors strongly preferred targeting smaller organizations in vendor compromise attacks. Eighty percent of all vendor compromise attacks targeted smaller organizations, with the technology industry being the primary focus across these attacks.

Vendor fraud attacks are becoming increasingly sophisticated as cybercriminals continue to use advanced techniques that bypass legacy security tools. In 2022, 56% of all threats bypassed legacy security solutions, indicating that organizations without proper security measures are at higher risk of these attacks and the negative impacts these attacks can have on the organization.
Business Workflows Involving User Data are Most Compromised

Significant disruptions, financial losses, and reputational damage to organizations are commonly the results of compromised business workflows. These attacks often involve bad actors infiltrating legitimate business workflows and altering sensitive business information, such as assigning new routing numbers for payment requests.

The Armorblox Research Team found that the most common types of compromised business workflow attacks seen across 2022 involved sensitive user data, such as user login credentials.

<table>
<thead>
<tr>
<th>Common Business Workflows Most Likely to be Compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensitive User Data</strong></td>
</tr>
<tr>
<td><strong>Confidential Organizational Data</strong></td>
</tr>
<tr>
<td><strong>Money</strong></td>
</tr>
</tbody>
</table>

- **52%** Sensitive User Data
- **34%** Confidential Organizational Data
- **14%** Money
Users rely heavily on email in order to accomplish the majority of their day-to-day tasks. Here are the most common email-based business workflows at risk of being compromised:

**Email Notifications**
Notifications from an email provider about mailbox status, e.g., email has been quarantined, a mailbox is full.

**Voicemail Notification**
Notifications to alert users of a voicemail that is pending to be reviewed.

**Password Reset**
Notifications from services that request password resets or updates to logins.

**Application Notification**
Notifications about shipments from Amazon, UPS, USPS, etc. or account alerts from AMEX and other providers.

**View Document**
Notifications asking users to review a document someone has shared with them.

---

**Compromised Business Email Workflow Trends**

<table>
<thead>
<tr>
<th>Workflow Type</th>
<th>2022 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Notifications</td>
<td>(30%)</td>
</tr>
<tr>
<td>Voicemail Notification</td>
<td>(22%)</td>
</tr>
<tr>
<td>Password Reset</td>
<td>(15%)</td>
</tr>
<tr>
<td>Business Application Notifications</td>
<td>(15%)</td>
</tr>
<tr>
<td>Viewing Document</td>
<td>(11%)</td>
</tr>
<tr>
<td>Other</td>
<td>(7%)</td>
</tr>
</tbody>
</table>
Over the first half of 2022, Armorblox found that business workflows involving email notifications were the most compromised, a significant uptick over 2021. As end users rely more heavily on email for business operations, we anticipate to see business workflows continue to be compromised by malicious actors.

Notifications from business applications are also fierce competitors for malicious actors to compromise. These include notifications advising users that an upgrade or current subscription renewal is needed for an associated account. These are common instances that end users legitimately come across – exactly why these workflows are some of the most compromised.

With organizations increasing security awareness and precautionary measures, it is no surprise that password reset workflows are also rising. When end users receive warning emails from trusted applications about malicious activity on their accounts, it is unlikely that the recipient will disregard the message. Bad actors take advantage of these email notifications’ severity to do more damage.
Language Remains Main Attack Vector to get BEC Attacks in Front of Employees

Business Email Compromise (BEC) attacks have become a significant threat to organizations in recent years, targeting businesses of all sizes and across industries. As BEC attacks continue to evolve, they are becoming increasingly sophisticated. Unfortunately, legacy security controls that rely on monolithic techniques, such as analyzing email headers, links, and metadata, enable these attacks to go undetected.

Data from the Armorblox Research Team suggests that the number of BEC attacks targeting organizations increased by 72% in 2022.

BEC Attacks by Industry

- **Education**
- **Nonprofit**
- **Software**
- **Travel & Leisure**
- **Tour & Games**
- **Shipping Logistics**
- **Financial**
- **HR**
- **Local & Storage**
- **Healthcare**
- **Telco Research**
- **Electronics**
- **Manufacturing**
- **Broadcasting**
- **Retail**
- **Real Estate**
- **Advertising**
Over the past year, Armorblox has seen attacks involving criminals posing as trusted individuals within the organization. These bad actors ask users to do a “quick task” or pose as trusted vendors to trick victims into sending money or paying a fraudulent invoice.
Language Remains Main Attack Vector to get BEC Attacks in Front of Employees

Across all BEC attacks seen over the past year, 57% relied on language as the main attack vector to get BEC attacks in front of unsuspecting employees. These attacks aim to get employees to steal money, pay fraudulent invoices, share user credentials, or exfiltrate sensitive organizational data.

In addition to high volumes of language-based and socially engineered attacks that plague organizations, we see a stark increase in graymail leading to malicious attacks. What once was only seen as a nuisance is now a fierce competitor in business email compromise. Armorblox saw 20% of BEC attacks fall within the graymail or unwanted solicitation category (up from just 4% the prior year).

Legacy solutions cannot accurately protect against malicious BEC attacks that use language as the primary attack vector. Coupled with the rise of BEC attacks disguised as graymail, there is genuine concern for the lack of protection against these sophisticated attacks legacy tools can provide organizations. Armorblox Research Team discovered that 77% of BEC attacks in 2022 bypassed these security layers.
Financial Industry at the Receiving End of Financial Fraud Attacks

Even with ongoing employee education and awareness programs, financial fraud attacks are still on the rise and are a concern for all organizations. For example, financial fraud attacks such as payroll, payment, and invoice fraud have increased by 72% over 2022.

Financial fraud attacks include a variety of broad-based attacks, with a large portion of advanced financial attacks not being captured by traditional security layers (22%). Native email security solutions fail to detect these sophisticated financial fraud attacks accurately due to evolving attack tactics, lack of context, limited NLU and ML capabilities, and the vulnerability legacy solutions create against unknown attack vectors.

The Armorblox Research Team took a deep dive into these financial fraud attacks. Of the total attacks that targeted our customer base, 22% of financial fraud attacks successfully bypassed native email security controls. Additional layers of protection and security measures that go beyond these security controls are crucial for organizations to implement for protection against these advanced financial fraud attacks that bypass these layers.
Financial Industry at the Receiving End of Financial Fraud Attacks

Evolving Tactics
Bad actors are constantly evolving their tactics to trick unsuspecting victims. For example, using social engineering techniques (such as impersonating a trusted vendor or third-party contact) can result in employees making wire transfers to fraudulent accounts.

These evolving tactics also make it difficult for legacy security measures to keep up, blindsiding these obsolete filtering tools and resulting in a malicious attack passing through.

Lack of Context and Machine Learning Capabilities
Legacy security tools rely solely on rule-based systems that are not capable of detecting subtle variations that separate legitimate business communications from financial fraud attacks. For example, without language-based models for context analysis, an email from a trusted executive requesting a wire transfer may not be flagged by the block-list model these legacy tools rely on.

Inadequate Threat Intelligence
With only access to the latest threat intelligence data, legacy solutions are vulnerable to zero-day and newly-discovered financial fraud attacks.

The continued rise in these attacks highlights the importance of implementing multi-layered security controls like Armorblox to defend against financial fraud.

Over the year, the most commonly targeted industries for financial fraud attacks included financial (49%), healthcare (40%), and education (11%).

Commonly Targeted Industries for Financial Fraud Attacks

- Financial (49%)
- Healthcare (40%)
- Education (11%)
In 2022, payment request attacks accounted for 89% of all email-based financial fraud attacks.

Looking deeper at financial fraud attack type trends per industry, Armorbox found that financial organizations are most likely to be targeted for invoice fraud (51%) and payment fraud (63%) attacks. Forty-nine percent of healthcare organizations were found to be at the receiving end of payroll fraud attacks.

Email-based financial fraud attacks commonly spoof common business workflows to steal money or gain access to accounts of targeted organizations.

Armorbox found that the most commonly spoofed financial-based business workflow is the request to pay an outstanding invoice. This attack typically starts with a bad actor impersonating a trusted vendor or third-party contact, sending a fraudulent invoice, and requesting payment as soon as possible.

If the bad actor succeeds, the targeted organization wires money directly into the bad actor’s bank account. In 2022, payment request attacks accounted for 89% of all email-based financial fraud attacks.
Financial Industry at the Receiving End of Financial Fraud Attacks

The following spoofed financial-based business workflows were seen in smaller volumes but can still result in significant financial losses and reputational damage to target organizations.

**Payment Requests:**
Individuals across departments commonly exchange email communications regarding invoices and payment requests. Bad actors know the frequency of business workflows is high and exploit this to execute financial fraud attacks that contain requests for inflated, duplicate, or fake invoices or transfer requests. The hope is that victims have seen these business workflows many times and will not hesitate to execute the request, resulting in a payday for the cyber thieves.

**Account Services Login Requests:**
For those who use work emails across business and personal apps, it is common to receive email alerts and notifications from these financial institutions. These logins are the only thing that separates them from their online bank accounts, and bad actors know that all it takes is one good bait to **phish**. By spoofing these common business workflows from financial institutions, bad actors hope that when victims get a fake email saying “your account is at risk,” they don’t think twice, opening that window of opportunity.

**Payroll Change Requests:**
These attacks happen when bad actors email an organization’s payroll, finance, or human resources department and impersonate a legitimate employee. Under this guise, they request an update to direct deposit information for future paychecks, usually asking that the change be made by the next pay cycle.
Malicious Actors Are Still Playing “Go Phish” with Legacy Solutions

Phishing attacks often involve criminals posing as trusted individuals to trick victims into revealing sensitive information. These include sending emails with links to fake landing pages or including illegitimate attachments that exfiltrate user credentials, or steal user and organization data. The Armorblox Research Team saw a 70% increase in phishing attacks in 2022, up from 63% the previous year.

Here’s a breakdown of zero-day phishing attacks seen across 2022 (see figure to right):

- 96% of total phishing attacks had malicious links within the email body
- 4% of all phishing attacks included illegitimate attachments

In 2022, there was a significant increase in zero-day phishing attacks, including malicious links within the email body (up from 85% of zero-day attacks in 2021). These attacks bypassed legacy tools, as language-based models cannot detect unknown, bad URLs.

The sheer increase in phishing attacks across organizations means that end users are more likely to be targeted in one of these attacks. And for organizations that rely on employees to spot and report all phishing attacks, simulations and training models are no match for these sophisticated, socially engineered attacks.

Zero-Day Phishing Attack Types

- 96% of total phishing attacks had malicious links within the email body
- 4% of all phishing attacks included illegitimate attachments
Malicious Actors Are Still Playing “Go Phish” with Legacy Solutions

Most Common Business Workflows Used within Phishing Attacks

- 52% of phishing attacks spoofed notification or alert workflows
- 40% of phishing attacks spoofed known IT requests, login, or user confirmation workflows
- 8% of phishing attacks spoofed password reset workflows

Bad actors craft targeted phishing attacks to look like business workflows that end users commonly use daily. These phishing attacks prey on the victims’ familiarity with these email workflows, hoping that end users will not hesitate before clicking a bad URL in a call-to-action button or hyperlinked text.

At 52% of all phishing email attacks, this places spoofed notification or alert workflows as the favorite among bad actors (up from 6% in 2021). This suggests that bad actors have pivoted, with the preference being to send phishing attacks pretending to be trusted business applications.

The data suggests an email that appears to come from Google Drive or Microsoft OneDrive suggesting storage is running out may be more likely to spark engagement from an end user than password reset emails, a spoofed workflow we see at the lower end (at only 8%) of all attacks.

Armorblox automatically classifies and detects email threats that target organizations. The Armorblox Research Team took a deep dive across these detection categories to identify the most significant email threats to end users. In 2022, credential phishing attacks comprised 51% of all targeted email threats.
Malicious Actors Are Still Playing “Go Phish” with Legacy Solutions

Breakdown of Email Threat Categories

- Social Engineering (41%)
- Credential Phishing (51%)
- VIP Impersonation (3%)
- Extortion (3%)
- Payroll Fraud (2%)

The increasing sophistication and social engineering behind these attacks make it hard for organizations relying solely on legacy security solutions to protect end users. Of all phishing attacks that targeted organizations in 2022, 78% used sophisticated techniques to successfully bypass native email security tools.
Lifting the Mask on Impersonation Attacks

Impersonation attacks are a growing threat to organizations, taking advantage of end-users' trust in executives, well-known brands, and vendor contacts. These attacks exploit this trust to trick unsuspecting victims into revealing sensitive information or sending money to fraudulent accounts.

Data gathered from the Armorblox Research Team reveals a significant increase in impersonation attacks targeting organizations across all industries. Our data shows a 38% increase in impersonation attacks in 2022 compared to the previous year.

In 2022, there was a 38% increase in impersonation attacks, compared to the previous year.
Lifting the Mask on Impersonation Attacks

Employee and VIP Impersonation Attacks

Employee and VIP impersonation attacks involve bad actors posing as trusted individuals within the victims’ organization, tricking employees into sending sensitive information, organizational data, or making a purchase due to an urgent request from an individual in power.

These attacks specifically exploit end users’ trust and willingness to please high-powered individuals. In 2022, Armorblox saw a 42% increase in both employee and VIP impersonation attacks.

There has been a notable rise in employee impersonation attacks, increasing by 40% in 2022. In these types of attacks, malicious individuals pretend to be trusted coworkers. End users that fall victim to these attacks put organizations at risk of bad actors obtaining access to sensitive information or confidential documents.

On the other end, data gathered from the Armorblox Research Team suggests that bad actors are still privy to targeting end users with VIP impersonation attacks. VIP impersonation attacks increased 33% in 2022. These targeted email attacks often fool loyal employees and play on their eagerness to abide by executives’ orders and expectations.
Lifting the Mask on Impersonation Attacks

In 2022, the Armorblox Research Team saw the following trends for employee vs. VIP impersonation attacks:

- 42% of all impersonation attacks imitated trusted Director-level and above employees across the organization
- 58% of all impersonation attacks imitated trusted VIPs across the organization
Lifting the Mask on Impersonation Attacks

Brand Impersonation Attacks
Brand impersonation attacks do not target just one industry or brand. These highly sophisticated attacks commonly involve emails and fake websites that mimic legitimate brands across the world’s largest organizations, like Zoom, DocuSign, Instagram, WhatsApp, and more.

These emails and websites are designed with one goal in mind – to trick recipients into providing sensitive information, such as usernames, passwords, and credit card numbers.

Over the past year, Armorblox saw a 74% increase in brand impersonation attacks.

Looking at the total brand impersonation attacks in 2022, the most impersonated brand, Microsoft, equated to almost 40% of all brand impersonation attacks. Interesting to note that the most spoofed brand in 2021 was Dropbox, which dropped from 38% (as seen in last year’s report) to 18% this year.
In 2022, 82% of all brand impersonation attacks bypassed native email security tools. Bad actors behind these attacks are not only perfecting the usual attack vectors, but are also expanding into new creative outlets to improve the validity of these attacks and gain the trust of their attack victims.

The Armorblox Research Team has noticed several brand impersonation attacks taking advantage of cloud-based email services, creating fake login pages for cloud-based applications such as Microsoft 365 or Google Workspace.

These pages trick victims into entering sensitive user credentials, which attackers can then use to access the victim’s email account. Email Authentication Checks such as SPF, DKIM, and DMARC help verify the authenticity of emails; however, bad actors have learned to use these standards to their advantage. By spoofing the email address of a trusted brand, they can now get past the very authentication checks created to detect and prevent these types of email attacks in the first place.
Smaller Organizations Are More Likely to Be Targets of Compromise Attacks

With the increasing reliance on email for personal and business communications, organizations must understand the current threat landscape and take necessary steps to protect themselves from compromise attacks. Additionally, the growing sophistication of these attacks has made email account compromise attacks a persistent and prevalent threat.

Email account compromise attacks are not slowing down. These attacks often involve unauthorized access and use of an individual’s email account, leading to compromised sensitive information, unauthorized transactions, and reputational damage to the affected organization.

Across 2022, the Armorblox Research Team found that suspicious logins were the most common signals of a potential account compromise.

![Most Common Signals of Potential Account Compromise](image)

- **38%** Suspicious Login Signals
- **24%** Unlikely Travel
- **12%** Suspicious Mail Forwarding Activity
- **26%** Other

Copyright © 2023 Armorblox Inc. All rights reserved.
The Armorblox team took a deeper dive into the total number of account compromise attempts that targeted organizations in 2022. Although account compromise attacks targeted organizations of all sizes, small-to-medium-sized organizations bore the brunt (with less than 10,000 employees). Over this past year, SMB organizations were the target of 58% of all account compromise attacks.
Smaller Organizations Are More Likely to Be Targets of Compromise Attacks

Additionally, from an organization perspective, data suggests that end users across Management, IT & Security, and Engineering departments receive the highest number of compromise attacks. This is most likely due to individuals within these departments having access to user- and organization-specific sensitive or confidential data.

<table>
<thead>
<tr>
<th>Department</th>
<th>Percentage of Compromised Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive</td>
<td>3%</td>
</tr>
<tr>
<td>Management</td>
<td>23%</td>
</tr>
<tr>
<td>Finance</td>
<td>4%</td>
</tr>
<tr>
<td>IT &amp; Security</td>
<td>17%</td>
</tr>
<tr>
<td>Engineering</td>
<td>17%</td>
</tr>
<tr>
<td>Sales &amp; Marketing</td>
<td>7%</td>
</tr>
<tr>
<td>Other</td>
<td>31%</td>
</tr>
</tbody>
</table>
Security Teams Waste up to 27 Hours a Week Managing Graymail Manually

Handling graymail not only requires time end users may not have to go through emails manually, but it also distracts users from identifying malicious emails. End users who quickly scan emails can easily mistake a malicious email for a genuine communication or outreach, potentially exposing their system to a cyber attack.

On the other hand, end users who report every suspicious email to the organization’s abuse mailbox create alerts that flood this mailbox with graymail that may be more annoying than harmful. This creates more manual work for security teams and increases the chances that a real threat will go unnoticed.

High volumes of graymail can present a potential security risk to organizations. Cybercriminals can use legitimate marketing emails as a cover to send malicious emails that may go undetected by end users or security teams. These emails may contain phishing links, malware attachments, or other forms of cyber attacks that can compromise the security of an organization’s network.

Across 2022, emails related to webinar or event promotions were the highest number of graymail flooding user inboxes at 33%.
Across 2022, the Armorblox Research Team looked at all graymail emails targeting end users and found the top three types of graymail most frequently hitting the inboxes of end users:

- 33% of graymail emails were event-related, including webinar or conference promotions and lists of event attendees
- 21% of graymail emails fell under the marketing and promotional category
- 20% of graymail emails included emails from HR and recruiting departments or about finances like real estate and loans.
Security Teams Waste up to 27 Hours a Week Managing Graymail Manually

Large numbers of graymail emails sent to users across the organization often result in security teams having to manually sort and delete these emails across user inboxes. This can lead to email overload, making it difficult for end users to identify and respond to important emails promptly. This can have serious consequences, particularly in industries such as healthcare or finance, where timely communication is crucial.

To bring this into perspective on the type of impact this can have across organizations, below we see the total number of hours it takes on average to manually remediate the graymail emails organizations receive.

For enterprise organizations, security teams can find themselves spending close to 30 hours a week manually remediating graymail emails.

Hours Spent per Week Manually Reviewing Graymail

- **2 Hours**
  - Small (Less than 1,000 employees)

- **7 Hours**
  - Medium (1,000 - 5,500 employees)

- **27 Hours**
  - Enterprise (Greater than 10,000 employees)
Data gathered from the Armorblox Research Team suggests that **large enterprises received 48% of all graymail emails sent to end users in the first half of 2022.** However, medium-sized businesses were not far off, receiving only 15% fewer graymail emails.
Methodology

Data for the report is based on information gathered from the following sources:
1. Armorblox threat research notes based on 58K+ customer tenants’ data.
2. Armorblox customer feedback, commentary, and insight on threat trends.

Definitions
- Year-over-Year growth: Calculated by comparing quarterly numbers during the same period across two different calendar years. For example, year-over-year growth was calculated by comparing 2021 H1 numbers to 2022 H1 numbers.
- BEC: Subset of customer threat incident data, including attack techniques leveraging social engineering and graymail or unwanted solicitation email attacks.
- Payroll Fraud: Subset of customer threat incident data that included wire fraud, invoice fraud, or vendor fraud due to email attacks.
- Financial Fraud: Subset of customer threat incident data that includes email threats related to internal and external payment fraud.
- Impersonation: Subset of customer threat incident data, including attack techniques leveraging brand and VIP impersonation.
- Phishing: Subset of customer threat incident data that included either a malicious URL in the body of the email or hidden within an email attachment to exfiltrate sensitive information.

Release Date: 04/11/2023
Lauryn Cash, Product Marketing, Armorblox

Armorblox Research Team:
Prashanth Arun, Head of Data Science
Anurag Shrestha, Data Engineer
Chuy Martinez, Jr. Data Analyst
Guilherme Osorio, Jr. Data Analyst