2022 Email Security Threat Report
Executive Summary

We are excited to bring you the first edition of the Armorblox 2022 Email Security Threat Report. This report offers IT and security leaders a deep understanding of the emerging threats, threat trends that happen over email, and highlights some of the significant changes in the threat landscape in the past year. We also provide a common reference point for defining commonly misused terms around the nature of these attacks so the industry has a framework for classifying these emerging threats. Here are some of the key insights that we discovered.

Key Insights

74%

Language based attacks have become the new normal for business email compromise (BEC). **3 out of 4 (74%)** business email compromise attacks **used language as the main attack vector.**

44%

Email-based financial fraud has become very sophisticated. **2 out of 5 (44%)** financial fraud attempts happen as **wire fraud, invoice fraud, or vendor fraud.**

87%

Attackers have realized that so many critical business workflows happen over emails, and this has become the primary attack mechanism for credential phishing. **9 out of 10 (87%)** credential phishing attacks looked like legitimate **common business workflows** in order to trick end users to engage with the email.

70%

Security teams spend a lot of time configuring rules and exceptions in their native email security solutions to block impersonation emails—both for executives and other employees. Despite all of that manual work and rule writing, **3.5 out of 5 (70%)** impersonation emails **slipped past native email security controls.**
State of Email Security Threats

Rise in Targeted Attacks
On May 3rd 2022, the FBI published a new report on Business Email Compromise. Based on reported complaints between June 2016 and December 2021, domestic and international exposed dollar losses due to business email compromise stands at $43.3 billion. And the volume of disclosed losses has exponentially increased year over year during this time period as well.

This also echoes the challenges that we hear from security teams—that despite increasing security budgets every year, email-based attacks still remain the #1 attack vector within organizations. We are witnessing a significant shift in the market landscape as well. The top two legacy email security vendors were both taken private by private equity firms in 2021, representing $1.5 billion in revenue. Several other legacy vendors were acquired and taken out of the market by larger players as well. These trends also indicate that legacy approaches are not working and too many attacks are slipping through.

Why is this? What has changed in how attackers target organizations? In this report, we highlight some of these significant trends. Attackers are moving away from tried and tested approaches from prior decades of using malicious links or attachments in broad based attack campaigns, to targeted attacks where the language in the email is used to compromise a user’s trust. This could manifest itself as fake wire transfer instructions, direct deposit change requests, password reset emails, or other common business workflows that happen over email. Whac-a-mole approaches of manual rule writing to block these newer attack types have remained unsuccessful and have caused repetitive, redundant, manual work for security teams. SOC teams have to comb through large volumes of potential phishing emails that users have reported to see which are legitimate emails and which need to be immediately deleted and removed from user mailboxes.

Moreover, as more security infrastructure moves into the cloud, security teams have become more loath to manually configure and maintain DNS and MX record rules to route emails through inline secure email gateways. This is also reflected in the 2021 Gartner Email Security Market Guide which states that 40% of all organizations will migrate towards modern API based email security solutions by 2023, the category that Gartner now calls Integrated Cloud Email Security (ICES).
Here at Armorblox, we protect over 58,000 organizations from targeted email attacks. We analyze over 2.5 billion emails a month, and stop over 500,000 threats every month. For this report, our threat research team looked at threat data from 2021, and compared it to the threats from the first quarter of 2022 to present the state of email security threats. The accompanying sections take a deep dive look into the four most prevalent threat types among the targeted email attacks - BEC, phishing attacks, impersonation attacks, and financial fraud.

“Systems that only analyze headers and metadata are not enough to reliably detect sophisticated threats like gift card scams or Business Email Compromise (BEC) attacks.”

– RUTHANNE BEVIER | Senior Information Security Advisor at Caltech
Executive Summary

State of Email Security Threats

Rise in Targeted Attacks
Business Email Compromise
Financial Fraud
Phishing Attacks
Impersonation Attacks
Brand Impersonation Attacks

Rise in Remote-Work Related Threats

Methodology

Business Email Compromise

Business Email Compromise (BEC) attacks are notoriously difficult to prevent. Attackers rely on social engineering techniques to persuade people into acting on the attacker’s behalf. As a result, traditional email security solutions that analyze email headers, links, and metadata often miss these attacks.

The number of BEC attacks targeting organizations increased by 74% in 2021.

Our research suggests that the number of BEC attacks targeting organizations increased by 74% in 2021. These BEC attacks target organizations across sectors and use language, malicious links, and common business workflows as the proxy to compromise employees and steal money, credentials, or sensitive data.

When researching the most prevalent strategies for BEC attacks over the course of 2021, we see the following trends (see figure).
One of the challenges in how BEC is used in the industry is that it represents a broad swathe of attack types. In addition to the socially engineered emails that pose an immediate threat, graymail is emerging as a category that can lead to malicious attacks. These are emails that look legitimate enough to bypass spam filters, and are sent without much regard to the CANSPAM Act. Bad actors use graymail as an attempt to identify which employees are out of office, and subsequently use the information provided within the out-of-office message to socially engineer email attacks to other employees. Graymail typically comes from generic email provider addresses such as @gmail.com or @outlook.com, making it hard to stop using traditional block list approaches.

BEC attacks that use language as the proxy to exfiltrate sensitive information is the main strategy malicious actors are using to target organizations. The use of language in BEC attacks has risen more than 53% year-over-year from 2021 to 2022, further supporting this strategy being favored among attackers.
Over 2021, bad actors relied on language as the main proxy for targeted BEC attacks. Language-based BEC attacks increase the chance of these sophisticated threats bypassing native email security controls and landing in the inboxes of unsuspecting employees. Of the BEC attacks that used malicious techniques to target organizations, 52% of BEC attacks were not caught by native email security controls.

“We see fraudsters crafting emails, prompting either for customers to take quick action, to send money somewhere, or to enter in their credentials. To combat these attacks we were looking for the kinds of smart features, like being able to look for emails that include language that is suggestive of fraud.”

– JONATHAN LEVINE | CTO of Intermedia
Financial Fraud

Email-based financial fraud attacks attempt to steal money from targeted organizations. The most common categories that we identified were payment fraud, vendor fraud, and payroll fraud.

- **Payment fraud attacks** are email attacks that contain requests for inflated, duplicate, or fake invoices or fake wire transfer requests.
- **Payroll fraud attacks** happen when attackers email an organization’s payroll, finance, or human resources department, impersonating a legitimate employee with a request to update direct deposit information for their paychecks.
- **Vendor fraud attacks** are the result of compromised third-party accounts, utilizing the trusted reputation of the vendor or end clients. These can also happen through vendor domain impersonation plus social engineering tactics in an effort to steal money and sensitive data.

**The Armorblox research team saw a 73% increase in financial fraud email threats year-over-year from 2021 to 2022.**

Organizations that communicate with vendors or third-party contacts can find themselves the target of financial fraud through compromised emails with trusted third party senders. These compromised communications are the result of impersonated vendor domains and emails. The vendor fraud attacks that equate to 25% of financial fraud attacks include the following three attack vectors: vendor domain spoofing, vendor account compromise, and vendor impersonation.
Healthcare, Education and Financial Service are the top three industry verticals that are affected by financial fraud in 2021. Between the three, the Financial Service industry was the target of 46% of these attacks (see figure).

These verticals also face unique email security challenges - they conduct business with large sets of vendors, facilitate email workflows that deal with money, and store large volumes of customer data.
Phishing is another broad category that combines several common types of attacks. Spear phishing refers to targeted attacks aimed at specific individuals, especially executives. Then there are the non-email phishing attacks - “vishing” that focuses on voicemail messages, “smishing” that tracks SMS based attacks, and even “quishing” that tracks the emerging category of QR code based attacks.

The phishing simulation and awareness industry focuses predominantly on training users to identify these kinds of attacks. Users get sent surprise phishing emails as part of a simulated phishing campaign and those unsuspecting users that click on the fake link get sent to take hours of training videos to get better. Studies show that despite five consecutive training sessions, 1 out of 7 users still click on the bad link.

As organizations work to protect their employees against common types of phishing scams, cybercriminals seem to stay one step ahead by adapting their tactics. Phishing attacks (including smishing and vishing) increased 63% year-over-year from 2021 to 2022. These sophisticated attacks mimic common business workflows, targeting and taking advantage of unsuspecting employees through social engineered payloads.
Bad actors target unsuspecting users with emails that include malicious URLs but look like legitimate common workflows. These phishing email attacks pry on the victims’ longing to participate in email workflows that they have commonly seen before without taking a step back to question authenticity.

In addition to phishing attacks that mimic common business workflows and rely on language as the main attack vector, our researchers saw an increase in zero-day phishing attacks. These email threats contained either a malicious URL within the body of the email or buried within an attachment (attachment types being HTML, PDF, or Word), easily bypassing legacy email security controls due to the creation of domains specifically for these phishing attacks.

85% of all zero-day phishing attacks in 2021 contained a malicious URL within the body of the email

Research corroborates that these attacks are harder to detect, and sophisticated email security solutions that process language as a signal are the key in detecting and protecting against phishing.
Impersonation Attacks

A form of Business Email Compromise (BEC), impersonation attacks have increased in effectiveness, leading to greater risk of victims engaging with them. For this report, we look at impersonation attacks across two categories: executive impersonation and employee impersonation. Bad actors do extensive research prior to executing an impersonation attack and aim to steal credentials or money and defraud organizations.

The Armorblox research team took a deep dive into executive and employee impersonation attacks seen over the past year to understand how they have evolved and to look at attack trends over the course of the year 2021.

Impersonation attacks increased by 29% year-over-year from 2021 to 2022

“Even with a SEG in place, we were getting emails impersonating the CMO and CEO, either asking for payments or just interrupting our employees’ daily work. This required us to manually go into the SEG and filter out these emails every time they appeared.”

– IT Manager at FinTech Company
Impersonation attacks are increasing, and bad actors are using these targeted attacks to steal sensitive information and money from organizations. We have seen executive impersonation attacks span from a bad actor pretending to be the CEO, sending an email from their Gmail account requesting corporate credit card details in preparation for a client meeting, to an, “Are you at your desk?” email turning into an iTunes gift card purchase request.

Over the past year, 70% of impersonation attacks slipped past native email security controls.

Due to the language-based nature of impersonation attacks, legacy email security controls that do not have language signals to detect targeted attacks cannot protect end users from these attacks. Research corroborates this, showing that 70% of impersonation attacks slipped past native email security controls in 2021.
Organizations cannot predict when employees will be the target of impersonation attacks; however, knowing attack trends by title and department can help determine which employees are most susceptible to receiving a suspicious email and which titles are most often impersonated during these attacks. In order to understand these trends, the research team at Armorblox took a look at the top departments that were the target of both executive and employee impersonation attacks over the course of the year 2021.

Looking across departments, Sales is most likely to be at the receiving end of an impersonation attack. Over the course of 2021, employees with the title VP, CTO, or CISO were the most targeted individuals. Attackers aim to gain sensitive business information through impersonation attacks, and impersonating employees that hold leadership positions can increase the chances of a victim complying with the request.
“Cities and counties have seen a startling increase in business email compromise and impersonation attacks.”

– ROB LLOYD  |  CIO of the City of San Jose

**Impersonation Attack Frequency by Season in 2021**

- Fall: 39%
- Summer: 28%
- Winter: 18%
- Spring: 16%

**Most Impersonated Brands in 2021**

- Dropbox: 38%
- Microsoft: 36%
- Docsign: 9%
- Other: 17%

Impersonation attacks are 2X more likely to happen in fall compared to spring.

Additionally, research shows impersonation attacks fluctuated in terms of frequency, depending on the season. Looking at one calendar year, organizations were the target of impersonation attacks the most during fall, two times more than compared to either winter or spring. During the fall season, the most targeted individuals within organizations were the executive leadership as well as the Sales department.

This data suggests that bad actors research the brands and applications that employees, within the target organization, use on a daily basis. This is in order to instill trust in the victim and create a sense of urgency for victims to engage with the email attack.
Rise in Remote Work-Related Threats

As organizations have shifted the way they work in the midst of the pandemic, cybercriminals have followed suit. With more reliance on email communication while working remotely, several new attack surfaces have opened up for cybercriminals to exploit. Socially engineered, targeted attacks have advanced, presenting a higher likelihood of getting past native security layers that still rely on manually configured rules and exception lists. Stopping targeted attacks requires custom models that understand good and bad patterns of communications in each organization using the content and context inside of email communications.

Most Commonly Spoofed Workflows

With the increase of remote work, attackers are dialing into the patterns of communication and common business-related email workflows employees engage in daily due to remote work, in order to craft targeted emails attacks.

We often forget how much of our daily jobs get done over email. Here are some:

**View Document**
These are emails that send us notifications asking us to review a document that someone has shared with us.

**Email Notifications**
These are notifications from the email provider about the status of our mailbox. Examples - Email has been quarantined, mailbox is full, etc.

**Application Notifications**
Examples are shipment notifications from Amazon, UPS, USPS. Or account alerts from Amex or other providers.

**Password Reset**
These are notifications from services that we use that ask us to reset or update our passwords.

**Voicemail Notifications**
These alert us to go listen to a voicemail or that our inbox is full.
We looked at threats detected between April and November 2021 to identify the most commonly spoofed email-based workflows. Here is what we found:

### Business Workflow Based Attacks in 2021

The first thing that stood out here was the sharp increase in app notifications. In a world where people are increasingly ordering things online, many confirmation and delivery notifications happen over email. We see mirrored trends when it comes to the volume of these attacks, with a rise in October and November as bad actors use these attacks to compromise people and steal credentials or money.

Password-related notifications have also been a very common way of compromising users to directly reveal their credentials to take over user accounts.

Email notifications that alert end users of unread voicemail messages have increased as a commonly spoofed business workflow over the course of 2021. Although we do not see a spike in these email attacks, like app notifications, the volume of these types of email attacks have increased over 2021, as bad actors continue to lean on this attack type to exfiltrate sensitive information.
Email-based business workflows are at the heart of how organizations operate today. A lot of the context around determining whether an email is legitimate or not does not reside solely in the headers and metadata any more. To effectively protect against targeted email attacks, the following characteristics are necessary in any effective email security solution:

1. Ability to look at historical data and identify good and bad patterns of communications.
2. Breadth of models to be able to track threats not just based on user identities and behavioral patterns, but also the language in emails to understand the content and the context of the communications.
3. Customizable models that can be trained to detect attacks in a particular organization, specifically based on communication patterns in that organization, as opposed to a horizontal approach that tries the same sets of rules and exceptions across all customers

The Armorblox Natural Language Understanding Platform accomplishes all this and more, to protect over 58,000 organizations against targeted email attacks and sensitive data loss.

For more information, visit https://www.armorblox.com/product/.
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 is calculated by comparing quarterly numbers during the same period across two different calendar years. For example year over year growth from 2021 to 2022 is calculated by comparing the Q1 numbers of 2021 and Q1 numbers of 2022.
- BEC - subset of customer threat incident data that included attack techniques leveraging social engineering and graymail or unwanted solicitation email attacks.
- Payroll Fraud - subset of customer threat incident data that include wire fraud, invoice fraud, or vendor fraud as a result of email attacks.
- Financial Fraud - subset of customer threat incident data that include email threats related to internal and external payment fraud.
- Impersonation - subset of customer threat incident data that included attack techniques that leveraged brand impersonation 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, with the goal to exfiltrate sensitive information.

Armorblox secures enterprise communications over email and other cloud office applications with the power of Natural Language Understanding. The Armorblox platform connects over APIs and analyzes thousands of signals to understand the context of communications and protect people and data from compromise. Over 58,000 organizations use Armorblox to stop BEC and targeted phishing attacks, protect sensitive PII and PCI, and automate remediation of user-reported email threats. Armorblox was featured in the 2019 Forbes AI 50 list and was named a 2020 Gartner Cool Vendor in Cloud Office Security. Founded in 2017, Armorblox is headquartered in Sunnyvale, CA and backed by General Catalyst and Next47.

To learn more about Armorblox, visit www.armorblox.com.

AUTHORS
Lauryn Cash, Sakthi Chandra, Anand Raghavan

ARMORBLOX RESEARCH TEAM
Anurag Shrestha, Prashanth Arun