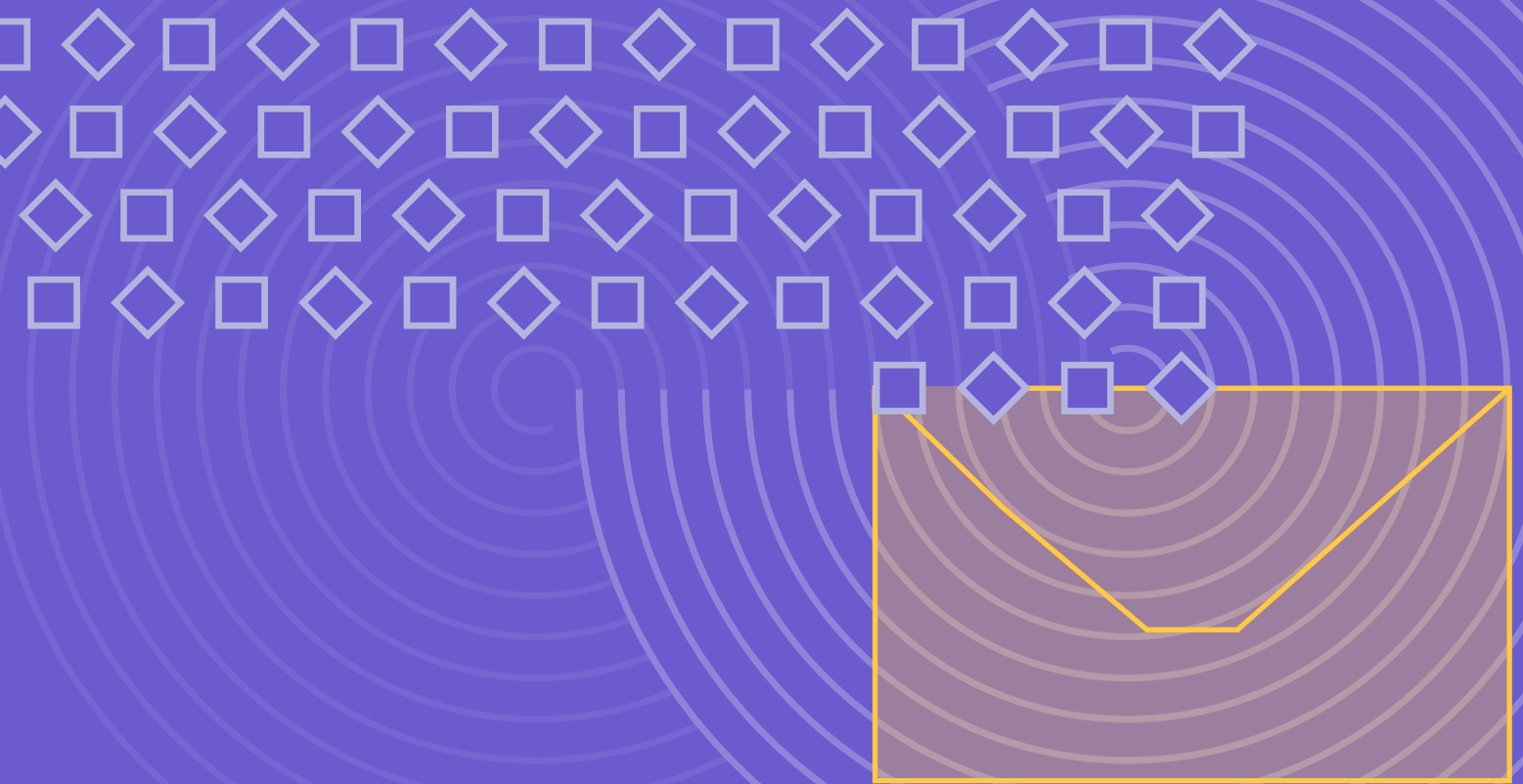


H2 2023 EMAIL THREAT REPORT

Applications Abound

Average Organization Now
Integrates 379 Third-Party
Applications with Email



Executive Summary

Email remains the most popular communications channel for legitimate business, and also the most targeted by cybercriminals. And with new advances in generative AI and the use of tools like ChatGPT, attacks have increased in both volume and sophistication over the past few months.

3,973

third-party applications installed on average for organizations with 30,000+ employees.

37.5%

of all third-party applications have high-risk permissions.

90%+

chance of receiving at least one BEC attack each week for organizations with 5,000+ mailboxes.

34%

increase in vendor email compromise attacks over previous two halves.

Massive Increase in Connected Third-Party Applications

Unfortunately, it's no longer simply inbound email under attack, as cybercriminals have started to shift their tactics. Third-party applications connected to the email environment are being exploited, and organizations are making the lives of bad actors easier as they continue to connect more applications with high-risk permissions.

With over **26,000** unique applications now connected across the Abnormal customer base, there has been a 128% increase in integrated third-party applications since 2020.

BEC and VEC Attack Volume Continues to Increase

Meanwhile, the number of both business email compromise (BEC) **and** vendor email compromise (VEC) attacks rose in the first half of 2023, continuing the trend we've seen over the last five years. By leveraging public information on websites, LinkedIn profiles, SEC disclosures, and more, cybercriminals can craft convincing, socially-engineered emails that deceive employees into sharing sensitive information or transferring money to attackers. In the first half of 2023, **BEC attacks increased by 55% over the previous six months**, and nearly half of all organizations have received at least one VEC attack since January.



Table of Contents

Attack Surface Area Widens with Increase in Connected Third-Party Applications	4
Email Threat Landscape Shifts in Early 2023	14
Steady Rise in Business Email Compromise Attacks	16
Vendor Email Compromise Increases and Evolves	20
Protecting Your Email from the Full Spectrum of Attacks	25
About Abnormal	26



Attack Surface Area Widens with Increase in Connected Third-Party Applications

For years, credential phishing links sent via inbound email were how attackers accessed email accounts. Proactive security leaders subsequently blocked this “front door” by implementing modern email security tools that detect those malicious links and prevent attacks from reaching end users.

Unfortunately, attackers have found new ways in, and are now using “side doors” in the form of connected third-party applications—allowing them to compromise email accounts without detection. The [recent attack on News Corp](#), parent company for *The Wall Street Journal* and *New York Post*, shows how even one connected malicious application can have disastrous consequences. In this case, the malicious application was connected to Microsoft 365 and stealing email data from key journalists for two years before it was discovered.

Third-Party Applications Pose a Risk to Your Email Environment

Vulnerabilities in third-party software accounted for 13% of all breaches in 2022—costing organizations an average of \$4.55 million per incident.

Source: IBM Cost of a Data Breach 2023



Application overload is a common and dangerous trend, particularly among distributed workforces that are leaning into the convenience and flexibility of cloud email platforms.

With dozens of plug-ins and third-party app integrations for everything from calendars to creative tools, even organizations with the most granular app policies may find themselves with security gaps. In fact, vulnerabilities in third-party software accounted for 13% of all breaches in 2022—costing organizations an average of \$4.55 million per incident.

There are a few ways that threat actors can use third-party applications to breach an organization. Common examples include:

- Stealing API keys and installing a malicious application with high-risk permissions.
- Using social engineering tactics to trick an internal user into installing what appears to be a legitimate application, but which actually provides the threat actor with access.
- Infiltrating the company that owns the third-party application and stealing data from its customers via the connected application.

These attacks are successful because they bypass traditional inbound email security tools—either because they have no apparent payload or because they do not have an email component at all.

So how can organizations detect and stop them? The key to stopping attacks that occur through connected third-party applications is by first understanding what applications are connected to email—and what those connected applications can do.

An Exponential Increase in Connected Third-Party Applications

379

applications are connected to organizations email tenants today.

Employees often connect to third-party applications via their email accounts in order to increase productivity and streamline workflows. But each time a user authorizes access to a new third-party application, they may be granting it the power to read and write emails, create calendar invitations, edit or delete company files, or manipulate data in other ways—all of which can put the organization's security at risk.

128%

increase in connected applications since 2020.

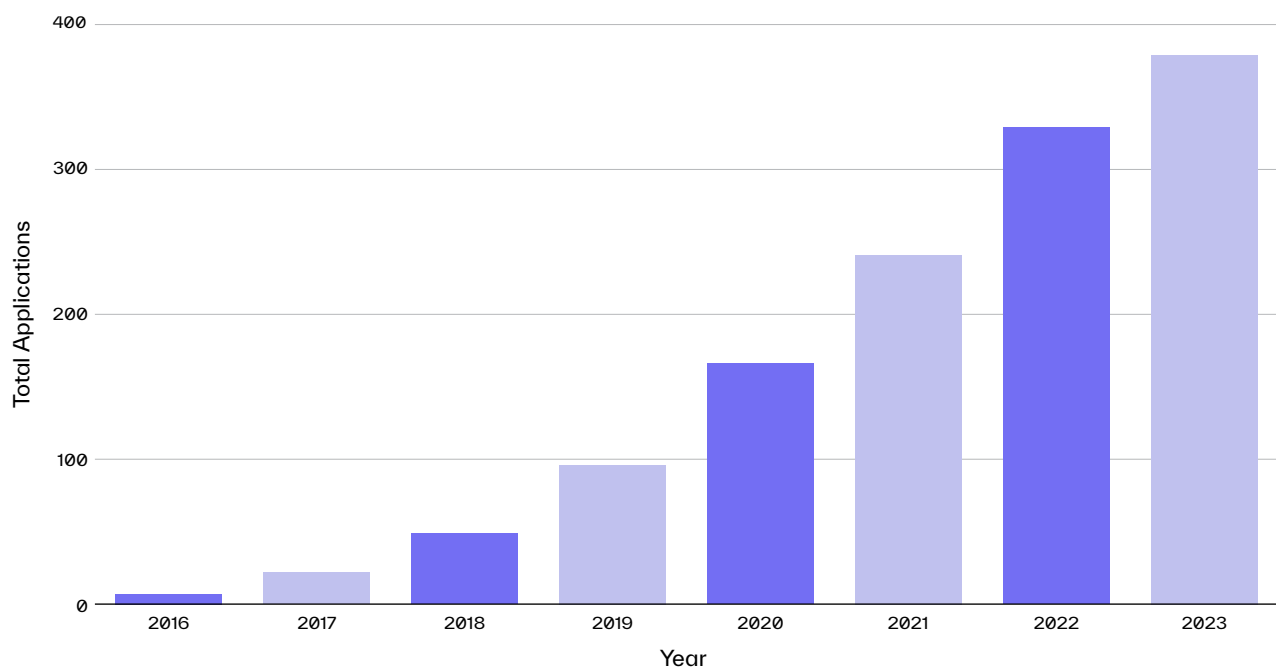
An Increase in Total Number of Connected Applications

The use of third-party applications is growing at an exponential rate, making it more difficult for security teams to understand the full scope of the problem. For example, the average organization today has 379 applications connected to their email tenant, compared to only seven applications in 2016.

In the last few years we've seen that number rise dramatically with a 128% increase in connected applications since 2020, when the average organization finished the year with 166 applications installed across the entire user base—less than half of what we see today.

Despite there being an average of 379 connected applications today, what is perhaps particularly concerning is that we're only halfway through the year. If the installations continue to grow on this same trajectory, we're likely to finish 2023 with more than 420 third-party applications installed per organization.

Average Number of Third-Party Applications by Year

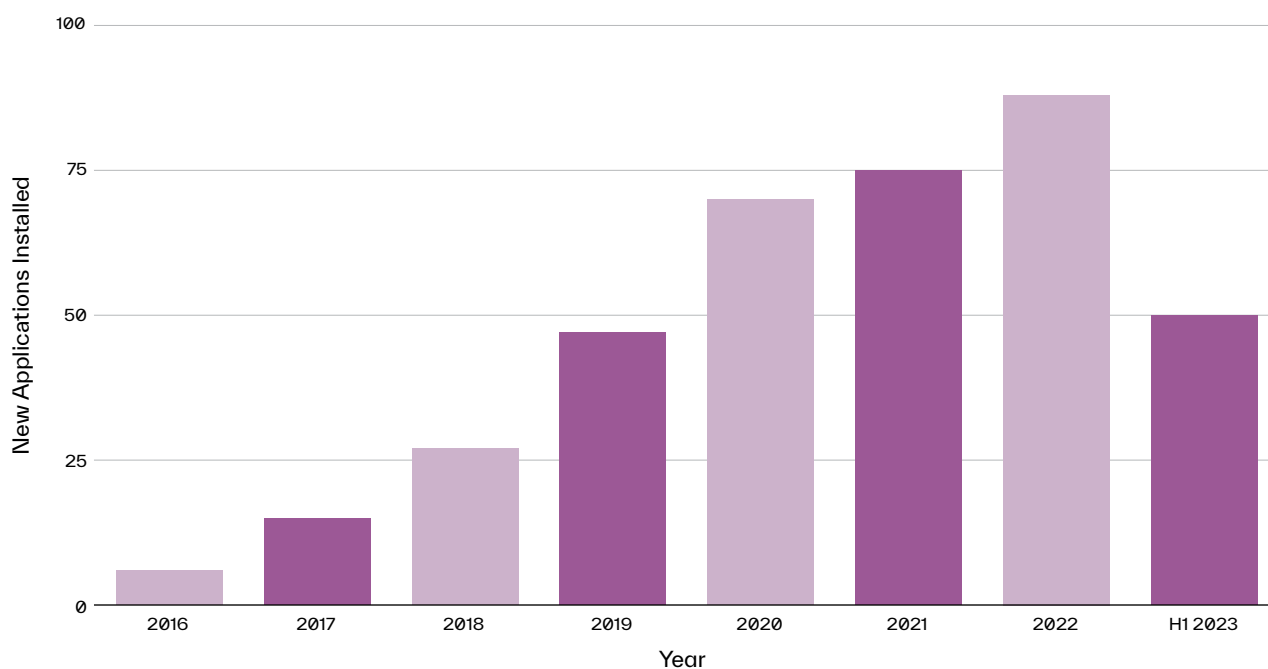


Number of New Installations Rises Each Year

Why is this number growing so quickly? Mostly because security teams and individuals alike are installing new applications at a rapid pace, without ever uninstalling the ones they're no longer using.

If we look at the number of new applications installed each year, that trend is very similar to what we see in the previous chart. In 2016, the average organization installed only six applications, but that number jumped to 88 last year and already reached 50 in the first half of 2023, an indication that new installations will hit triple digits by the end of the year.

Average Number of Third-Party Applications Installed Each Year



What does all this mean? That the threat surface is ever expanding, and security leaders must understand what is being installed in order to understand which applications may be risky. Without a clear picture of the total number of third-party applications connected to the email tenant, any one of them could have been installed for malicious purposes—or could be used in a malicious way moving forward.

3,973

third-party applications installed on average for organizations with 30,000+ employees.

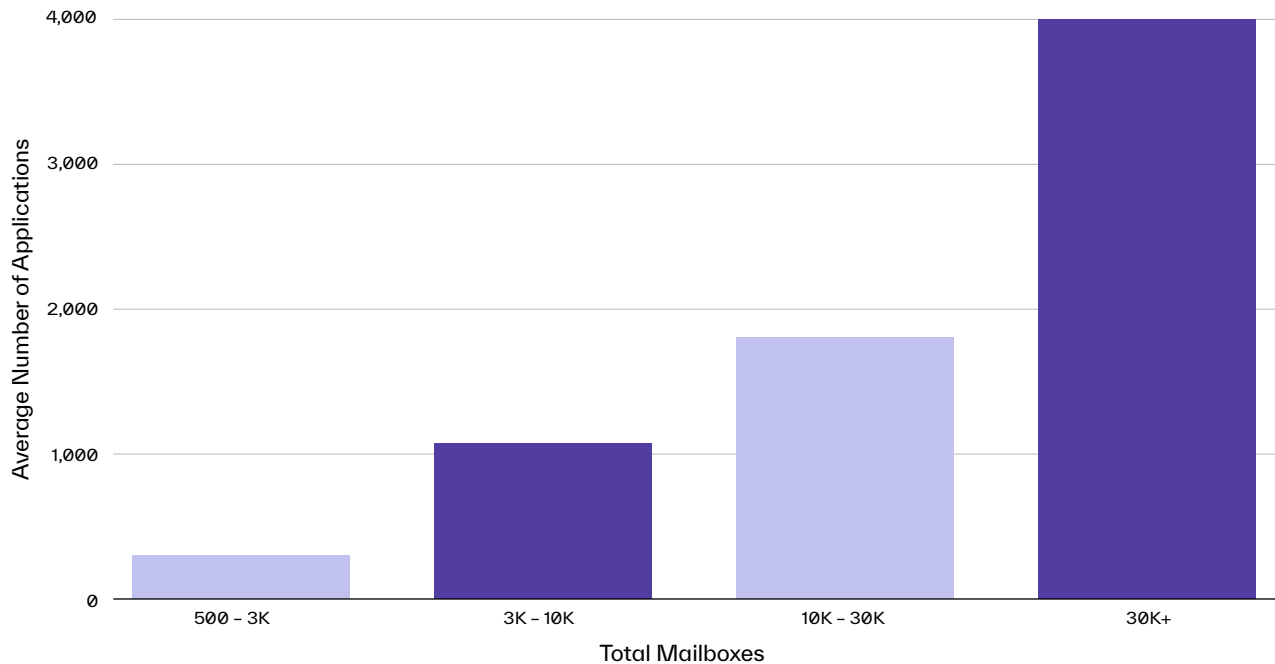
An average of about one application per 23 users.

Larger Organizations Have Larger Application Threat Surface

Perhaps unsurprisingly, those organizations with more employees have drastically more applications installed. This is likely because each individual has different needs and, in most cases, the opportunity to connect their email accounts to any third-party application they choose. As the organization grows, it only makes sense that more people will install a larger number of applications for everything from video conferencing to calendaring to project management.

What is surprising, however, is simply **how many** applications the largest organizations have installed—an average of nearly 4,000 for those companies with 30,000+ employees. On the other end of the spectrum, we see an average of nearly 300 applications for organizations with fewer than 3,000 mailboxes.

Average Number of Applications by Organization Size



Overall, we see an average of about **one application per 23 users**, showcasing how prevalent third-party applications actually are within the enterprise ecosystem—and why these connected applications are an issue no matter how large your organization is.

Organizations Install Thousands of Different Third-Party Applications





















Across the Abnormal customer base, more than 26,000 applications have been connected to more than one email tenant—underscoring the many ways threat actors can access email environments.

26,000+

applications connected to more than one email tenant across the Abnormal customer base.

Types of Third-Party Applications

But in addition to looking at the quantity of applications, it's important to understand the type of applications connected. A majority of applications are ones you'd expect to see in a business environment: development, collaboration, conferencing, and project management. A few of the most common third-party applications, connected to the email tenants of at least 80% of Abnormal customers, include:

Application	Category	Application	Category
 Zoom	Collaboration	 polly.ai	Collaboration
 SmartSheet	Collaboration	 AddEvent	Calendar
 Azure	Development	 Atlassian	Collaboration
 Apple Internet Accounts	Productivity	 Office 365 Service Communications API	Security
 Graph Explorer	Development	 Samsung Email	Productivity
 Neptune DXP	Development	 Cisco WebEx Scheduler	Calendar
 Adobe Acrobat	Productivity	 Calendly	Calendar
 LinkedIn	Social Media	 Rocketbook	Productivity
 Office 365 Shell WCSS-Client	Security	 Salesforce	Productivity
 SurveyMonkey	Productivity	 Jira Cloud	Productivity

These top applications are owned by some of the most well-known and well-trusted brands. Unfortunately, the reliance on them means that should one of them suffer a breach, malicious actors could have access to the email of millions of organizations.

Risk Levels Vary Across Third-Party Applications

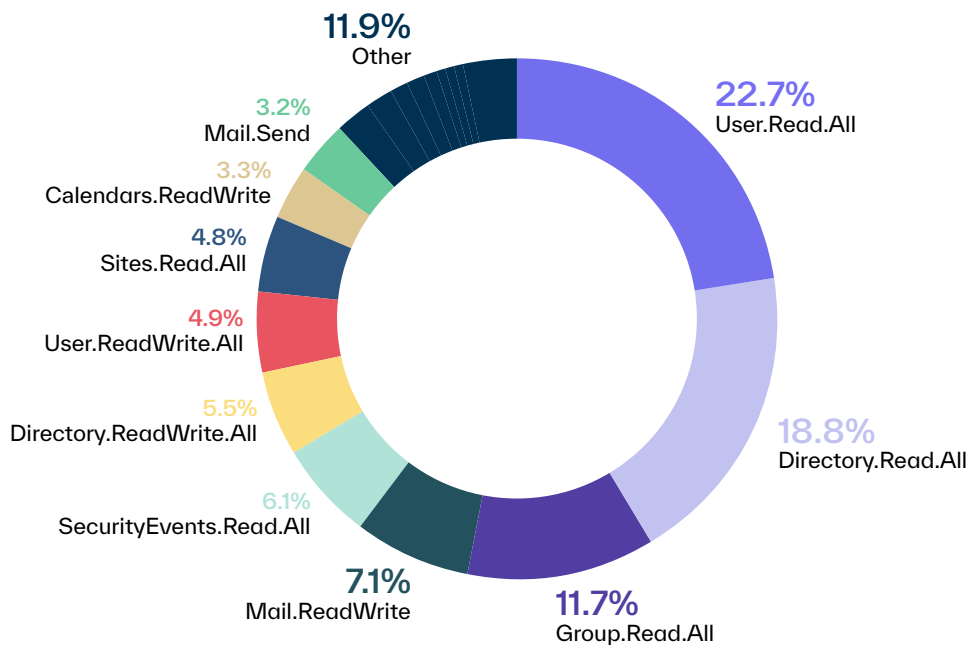
Each third-party application is a potential entry point into your email environment, but not all applications are created equally. The permissions provided to each application vary, and it's important for security teams and end users alike to understand what they're agreeing to when they install a new app.

Third-Party Applications Request a Wide Variety of Permissions

When third-party applications are connected to the email tenant, they ask for permissions for a number of use cases. Some of these permissions are fairly innocuous, like reading a calendar—which is likely not going to provide access to sensitive information. Others hold a medium amount of risk, like giving read access to email content, which is where sensitive business information is often stored. But there are also high-risk permissions, like those that enable an app to create and delete content within the mailbox.

Of the applications installed into the email tenants of Abnormal customers, the 10 most common tenant-level permissions make up 88% of permissions requested across all applications.

Tenant-Level Permissions Across Third-Party Applications



To understand the impact of these permissions, it's important to know what the permission allows and which applications ask for that permission. **The top ten most common permissions are as follows:**

Permission/Description	Example Applications	Percentage of Permissions Across Installed Applications
User.Read.All ● Medium Risk Allows the app to read user profiles without a signed-in user.	Zoom, Rubrik, SharePoint, Cisco Webex Scheduler, Postman	22.7%
Directory.Read.All ● Medium Risk Allows the app to read data in the organization's directory, such as users, groups, and apps, without a signed-in user.	Smartsheet, Netskope	18.8%
Group.Read.All ● Medium Risk Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.	Atlassian, Backupify, Gong, Elastic	11.7%
Mail.ReadWrite ● High Risk Allows the app to create, read, update, and delete mail in all mailboxes without a signed-in user. Does not include permission to send mail.	Samsung Email, Skykick Backup, PhishER, LogicHub	7.1%
SecurityEvents.Read.All ● Medium Risk Allows the app to read the organization's security events without a signed-in user.	Cisco, Expel O365 Integration, Bytes Quantum Health Check, Trend Micro Vision One	6.1%
Directory.ReadWrite.All ● High Risk Allows the app to read and write data in the organization's directory, such as users and groups, without a signed-in user. Does not allow user or group deletion.	Azure, Metallic Backup App for Exchange Online, SailPoint	5.5%
User.ReadWrite.All ● High Risk Allows the app to read and update user profiles without a signed-in user.	Salesforce, Moodle, CodeTwo User Photos for Office 365, Druva M365 Advanced	4.9%
Sites.Read.All ● Medium Risk Allows the app to read documents and list items in all site collections without a signed-in user.	Office 365 Mover, Backupify	4.8%
Calendars.ReadWrite ● High Risk Allows the app to create, read, update, and delete events on all calendars without a signed-in user.	Calendly, Clearrooms Calendar Integration, BetterCloud	3.3%
Mail.Send ● High Risk Allows the app to send mail as any user without a signed-in user.	AvePoint Teams Governance, ShareGate Teams Management	3.2%

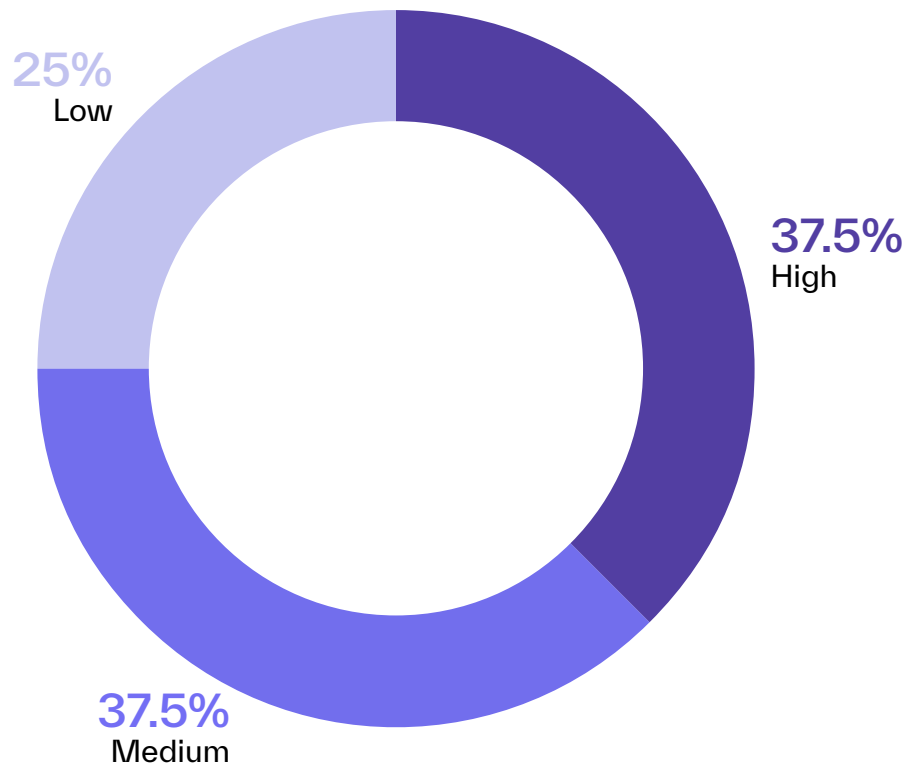


As you can see, some of the most common permissions also allow some of the largest access—enabling third-party applications to create and delete emails, create and delete users, and even reset user passwords. Perhaps most concerning about this is that these permissions are applied tenant-wide, so applications have the same permissions not just for one user, but across the entire organization.



Of the top thirty permissions seen by Abnormal, more than 37% are considered high-risk, while that same amount are considered at least medium risk to the organization.

Risk Level of 30 Most Common Permissions



Of the top 30 most common app permissions, 75% are considered medium or high risk.

Notably, only a quarter of the 30 most common permissions are low risk, underscoring how important it is for security teams to understand which applications are connected to email and what permissions they've been given.



Deep Dive into High-Risk Permissions

Unfortunately for security leaders, it only takes one rogue application to cause harm, so it's important to be extra cautious of those applications that request high-risk permissions. In some cases, employees may give an application one of these permissions without ever knowing what they're installing.

As such, in addition to those mentioned above, other high-risk permissions to keep an eye on include:

Permission	Description
CallRecords.Read.All	Allows the app to read call records for all calls and online meetings without a signed-in user.
Teamwork.Migrate.All	Allows to create chat and channel messages with anyone's identity and with any timestamp.
TeamMember.ReadWrite.All	Allows the app to add and remove members from all teams, without a signed-in user. Also allows to change a team member's role, for example from owner to non-owner or vice versa.
AdministrativeUnit.ReadWrite.All	Allows the app to create, read, update, and delete administrative units and manage administrative unit membership without a signed-in user.
AppRoleAssignment.ReadWrite.All	Allows the app to manage permission grants for application permissions to any API (including Microsoft Graph) and application assignments for any app without a signed-in user.
DelegatedAdminRelationship.ReadWrite.All	Allows the app to manage, create, update, and/or terminate Delegated Admin relationships with customers and role assignments to security groups for active Delegated Admin relationships without a signed-in user.

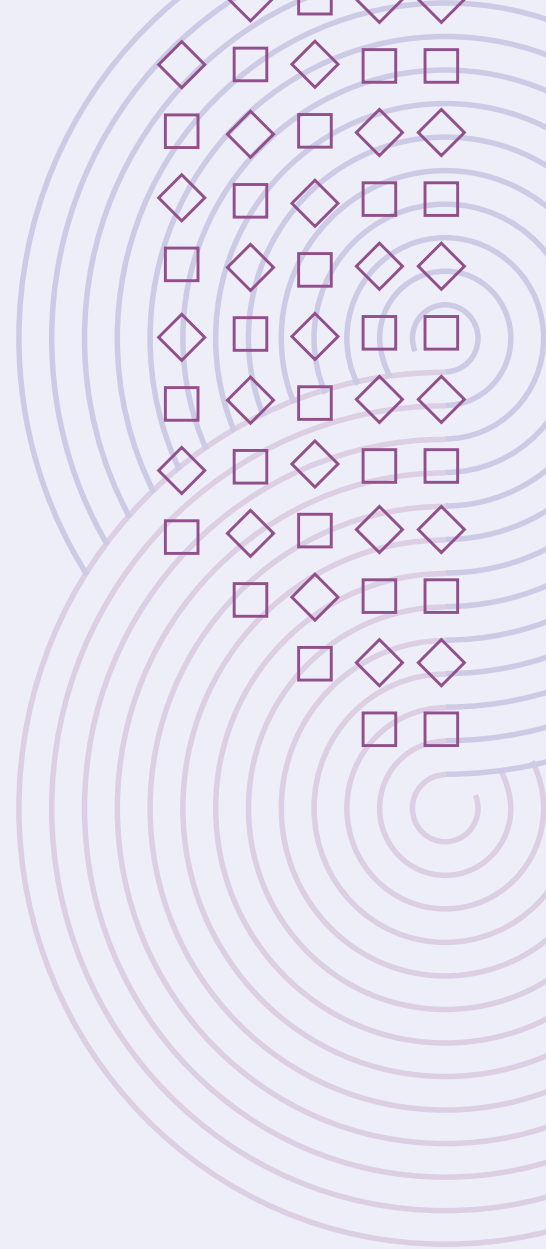


The moral of the story? With hundreds (or thousands) of applications connected to your email tenant, it's vital to know **what is connected and why**. Each application provides another side door into your email, enabling threat actors to infiltrate your organization—likely without you ever knowing. Understanding what applications are connected, knowing which permissions they have, and monitoring for configuration changes can help you ensure that your organization is staying protected from all types of email attacks—even those bypassing your inbox.



Email Threat Landscape Shifts in Early 2023

Email remains a favorite channel for cybercriminals to infiltrate organizations, despite an increase in both security awareness and advancements made by legacy security tools. Why? Because it's **still** one of the easiest ways to infiltrate organizations. There are simply too many people who click on a phishing link, respond to an email, or send money to the wrong person once a malicious email lands in their inbox.



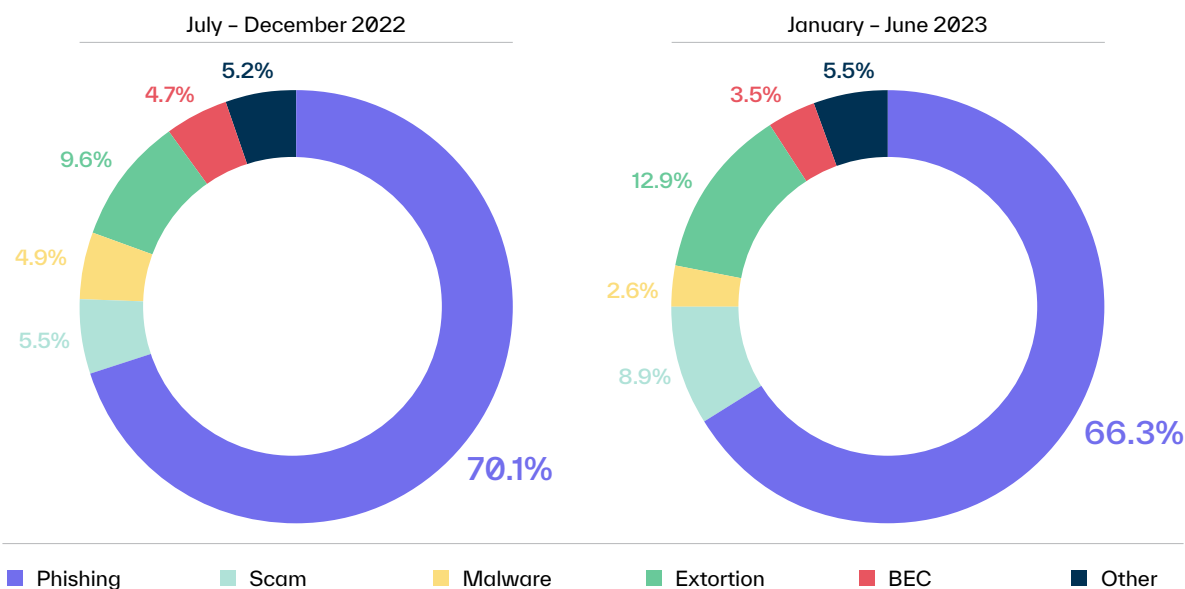
BEC Overtakes Malware in First Half of 2023

Phishing accounts for nearly 2/3 of all advanced inbound email attacks.

Over the past year, the number of attacks has grown but the type of attacks has shifted—demonstrating how rapidly the threat landscape can change, and how quickly threat actors will shift their tactics.

Unsurprisingly, given the fact that credential phishing provides opportunities to run almost any other attack, phishing is still the most common email attack type—accounting for 66% of advanced attacks in the first half of 2023. This represents a slight decrease from the 70% seen in the previous six months. This shouldn't suggest that phishing is declining, though, as it remains a fan (or threat actor) favorite.

Percentage of Advanced Attacks by Type



25%
decrease in BEC as a percentage of all attacks in H1 2023.

Perhaps more interesting is the fact that business email compromise overtook malware as a percentage of all attacks, a reversal from previous trends. If threat actors are investing more time and energy into BEC this year, it could be a result of the introduction of ChatGPT, which is allowing them to create more sophisticated attacks at a higher volume than ever before.

In addition, extortion jumped in proportion, and scams similarly took up a bigger slice of the pie over the previous six months. Threat actors regularly modify their tactics to improve their chances of successfully compromising their targets—making it vital for security teams to secure their email environments from the full spectrum of attacks.





Steady Rise in Business Email Compromise Attacks

Unfortunately, the rise in attacks that target email through third-party applications has not reduced the number of inbound email attacks that target organizations. It simply means that there are more surfaces to protect, and more ways for threat actors to gain access, steal money, and extract sensitive data.

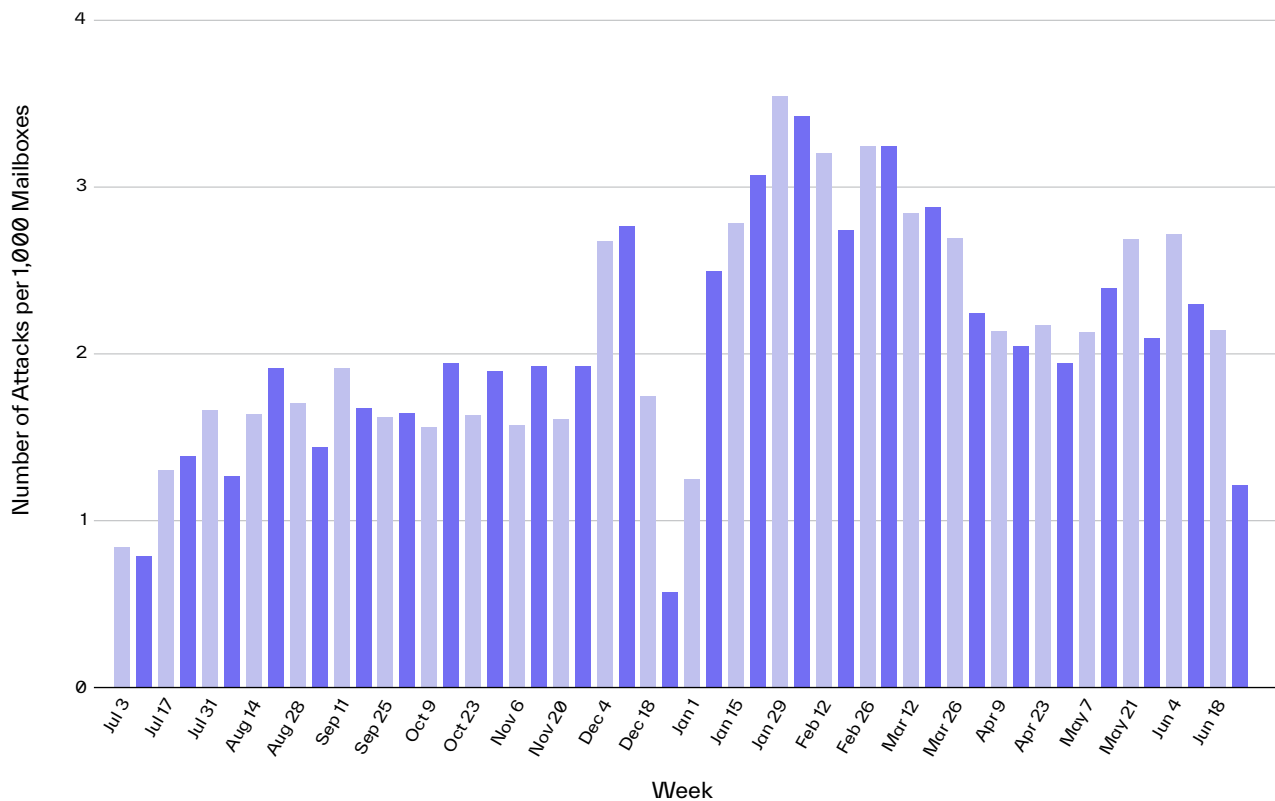
Business email compromise remains the most financially devastating threat to organizations for the eighth straight year, and we saw a notable surge over the previous six months. As mentioned above, this sophisticated type of email attack is beginning to outpace malware delivery, signaling a shift in the threat landscape.

BEC Attacks Increase Significantly in Early 2023

Business email compromise attacks—known for their reliance on text-only emails and social engineering tactics—grew in volume by 55% over the last six months.

This is an increase from 1.63 attacks per 1,000 mailboxes in the latter half of 2022 to 2.52 attacks over the first half of this year. Underscoring this increase is the fact that only a few years ago, the number of BEC attacks was much lower—averaging less than one attack per 1,000 mailboxes each week.

Median Weekly BEC Attacks per 1,000 Mailboxes



Following the holiday dip common at the end of December, BEC attacks jumped to 2.49 attacks per 1,000 mailboxes in the week of January 8th. From there, threat actors continued to send even more attacks—peaking in the week of January 29th with 3.55 attacks per 1,000 inboxes.

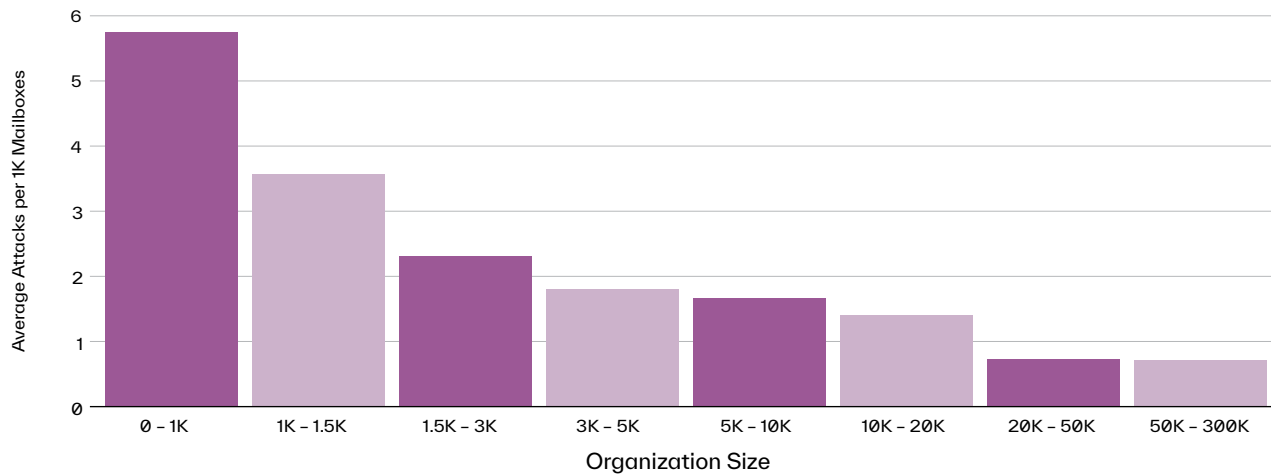
This heightened attack level held steady until early April when the rate of attacks fell to 2.1 attacks a week—perhaps when bad actors started to scale back their efforts to enjoy the summer. Even then, this relative decrease is above the average rate recorded in the second half of 2022.



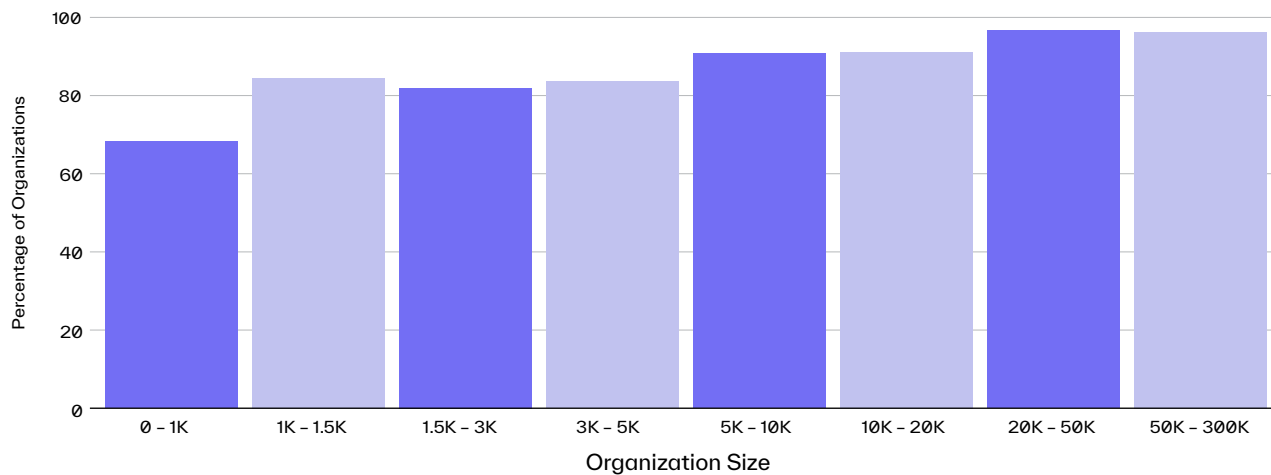
BEC Attacks Vary by Organization Size and Industry

Organizations with fewer than 1,000 employees saw the highest number of BEC attacks with 5.75 attacks per 1,000 mailboxes over the first half of 2023. However, the largest organizations, comprising more than 50,000 employees, experience a higher probability (96.3%) of receiving at least one BEC attack each week. While this might seem counterintuitive, the largest organizations simply have more mailboxes for possible incursion. And since BEC attacks are typically very targeted, smaller organizations receive more of them per employee each year.

Average Number of BEC Attacks by Organization Size



Percentage of Organizations Receiving a BEC Attack Each Week by Organization Size



This presents difficulties for organizations of all sizes. Attackers see small companies as potential soft targets due to their limited resources. On the other hand, large organizations are simply a numbers game.



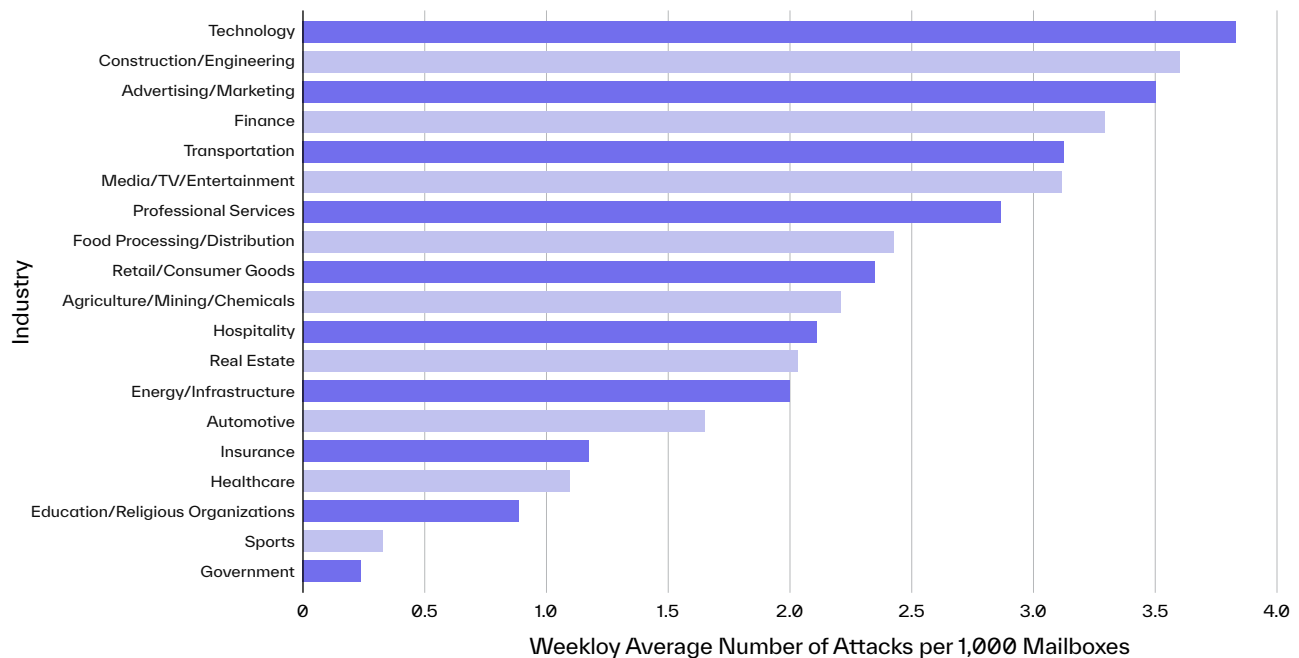
Technology, Construction, and Advertising Industries Prioritized for BEC Attacks

The technology industry saw an weekly average of nearly 3.85 attacks per 1,000 mailboxes.

BEC is on the rise across the board, but the number of attacks is not evenly distributed across industries. While the attack type is fairly industry-agnostic, cybercriminals may focus on a few industries where they've seen previous success or that have fewer security measures in place.

The technology industry is the most popular target for BEC attacks by far, with a weekly average of nearly four attacks per 1,000 mailboxes over the last half. This industry in particular is very innovative with a rapidly growing market, composed of organizations that house valuable intellectual property. And due to its constantly evolving landscape, attackers may believe that they can exploit vulnerabilities in these ever-changing processes.

Average Weekly Number of BEC Attacks by Industry



Other popular industries included construction, advertising and marketing, finance, transportation, and media/entertainment—all with over three weekly attacks per 1,000 mailboxes. Each of these industries faces its own unique challenges. For example, construction and engineering firms handle large transactions often in the millions of dollars. And marketing agencies work with hundreds of different customers and partners, perhaps making it easier for threat actors to gain access.

Vendor Email Compromise Increases and Evolves

As business email compromise has evolved, threat actors have identified vendors as the weakest link in the system—targeting their email accounts and using the information contained within them to infiltrate customers and partners.

Known as vendor email compromise, these attacks are particularly dangerous due to their ability to mimic legitimate vendor communications or hijack real conversations to encourage recipients to update banking account information or send fraudulent payments. The cost of these attacks to businesses can be frightening, strain relationships with customers and partners, and severely slow down operations.



VEC Attacks See Slight Escalation

\$36 million

requested in the largest VEC attack blocked by Abnormal.

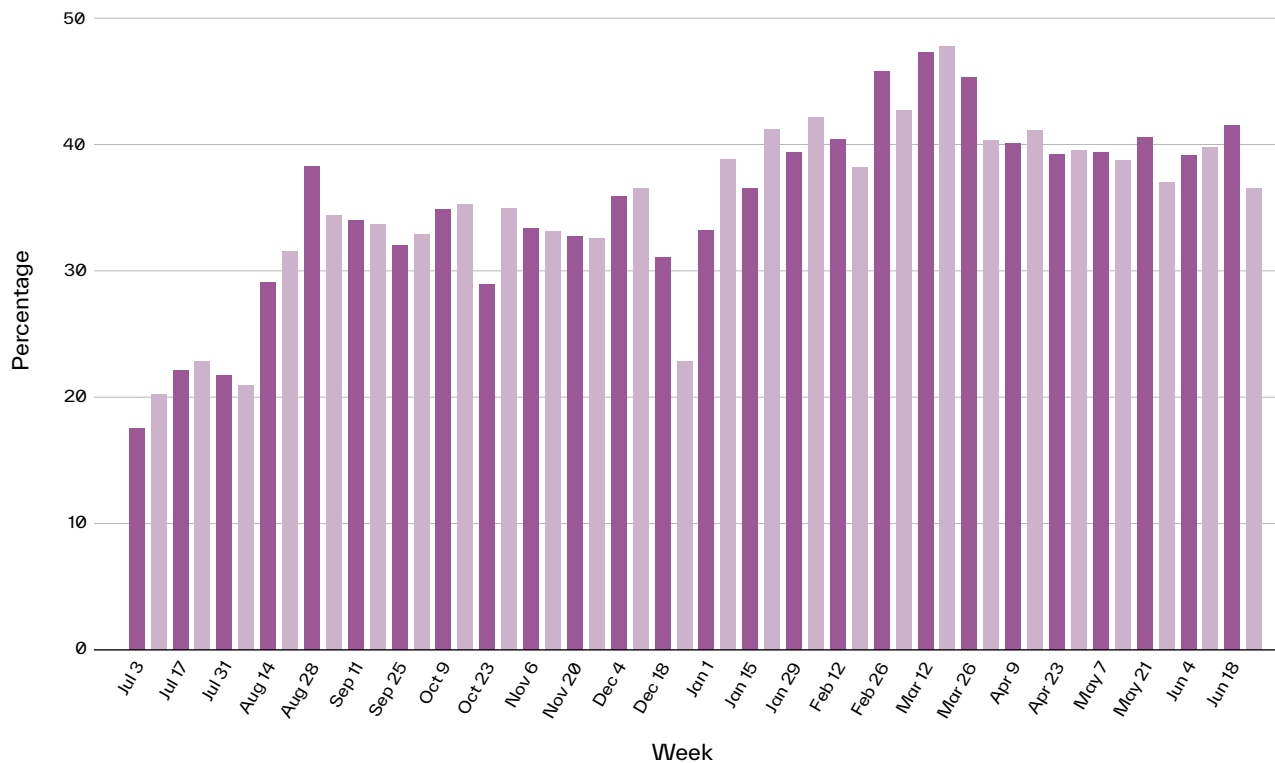
48%

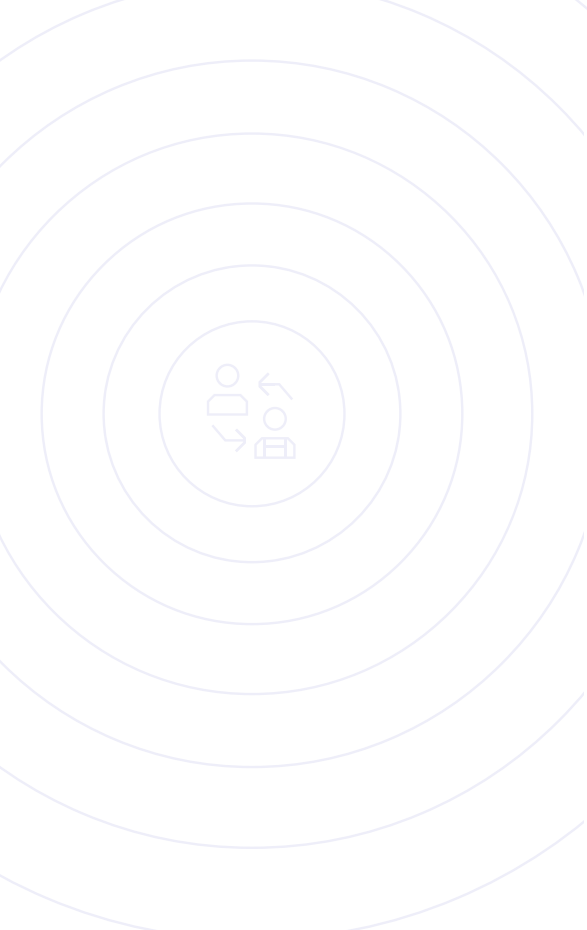
of organizations received a VEC attack in the first half of 2023.

Vendor email compromise is a type of business email compromise in which the malicious email is sent from a vendor or partner, rather than an executive or internal employee. The objective of these attacks is typically financial, where the attacker asks the target to send payment for an invoice or make updates to billing account details. Most of these attacks request less than \$150,000 but there are some that can cost millions in damage—including a **\$36 million VEC attack** recently stopped by Abnormal.

Because these attacks are **highly** targeted and rely on specific details related to vendor-customer relationships, they are not quite as prevalent as executive impersonation attacks that request gift cards or updates to payroll. That said, threat actors appear to be putting additional effort into their email threats, as 48% of organizations received a VEC attack this half—an increase from 45% in late 2022. And as more people become aware of the executive impersonation attacks that plagued organizations over the past few years, attackers may be increasing their reliance on vendor impersonation to avoid detection.

Percentage of Organizations Receiving a VEC Attack Each Week





VEC attacks have consistently grown since the COVID-19 pandemic, when cybercriminals exploited supply chain issues and reliance on email communication to mask their attacks. As the economy slumps in early 2023, many businesses trimmed their spending and headcount, which ultimately created vulnerabilities as processes, technologies, and staffing fluctuated. Further, remaining and incoming employees might lack historical knowledge about their vendors—creating new opportunities for attackers.

To complicate matters further, the launch of ChatGPT in November 2022 has helped attackers produce [high-quality email copy](#). By feeding the AI tools examples of the vendor’s tone and previous communications, attackers can more aptly impersonate legitimate vendors to fool their victims.

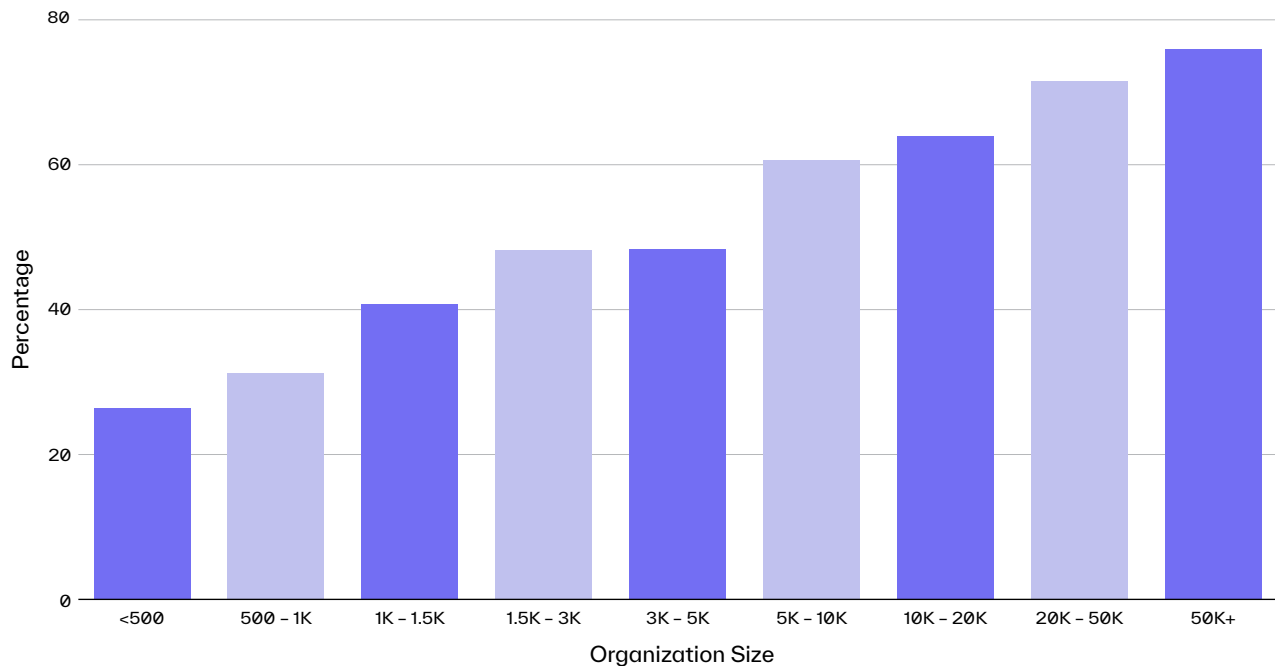
As new technologies are leveraged by attackers and the threat continues to evolve, it is crucial for organizations to remain vigilant, educate employees about potential risks, and implement robust cybersecurity measures to protect against VEC attacks and other types of vendor impersonation.

Most VEC attacks request less than \$150,00 but there are some that request much more—including a \$36 million invoice fraud attack recently stopped by Abnormal.

VEC Attacks Target Larger Organizations with Increased Frequency

Because VEC attacks are highly targeted and require access to a vendor account, they are more likely to target larger organizations with more vendors.

Percentage of Organizations Receiving a VEC Attack by Organization Size



76%

of organizations with more than 5,000 employees received a VEC attack in the first half of 2023.

Likely due to the fact that they have fewer vendors, smaller businesses are less likely to receive a VEC attack. The risk for larger enterprises with a workforce of 5,000+ is considerably higher, with VEC attacks targeting 76% of those organizations over the first half of 2023. This is an increase from last half, where only 67% of these large organizations received one or more VEC attacks over the course of the half.

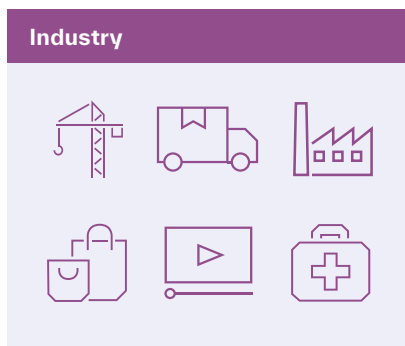
Since organizations rely heavily on partners, vendors, and suppliers, the threat of VEC will remain ever present—and will likely increase as threat actors see more success. Unfortunately, due to their sophisticated nature and use of legitimate (compromised) email accounts, these attacks can be nearly impossible for humans to detect.



All Industries Susceptible to Vendor Email Compromise

Nearly 77% of all companies in the advertising and marketing industry received a VEC attack in the first half of 2023.

Companies of all sizes and industries are vulnerable to VEC attacks, but cybercriminals still have their preferred targets, with the advertising and marketing industry receiving the most attacks in the first six months of the year. Since marketers and advertisers rely heavily on software as a service (SaaS), partners, and events, attackers see a plethora of opportunities to maliciously mimic real vendors.



Industry	Percentage of Companies Targeted (January - June 2023)
Advertising/Marketing	76.9%
Agriculture/Mining/Chemicals	71.4%
Food Processing & Distribution	69.8%
Construction/Engineering	69.0%
Transportation	69.0%
Automotive	67.7%
Retail/Consumer Goods	67.1%
Energy/Infrastructure	66.0%
Media/TV/Entertainment	65.0%
Healthcare	54.6%

Other popular industries targeted include agriculture, food processing, engineering, transportation, and retail—all of which rely heavily on vendors across the supply chain to run their businesses.

Unfortunately, as businesses rely more on their vendors and attackers recognize how much success they can have, these numbers are only going to increase. All industries should be prepared, but these in particular should implement the security tools necessary to keep VEC attacks from reaching employee inboxes.

Protecting Your Email from the Full Spectrum of Attacks

Whether bad actors attack through the front door with an inbound email or through a side door via a connected third-party application, organizations must be prepared to defend against them. Inbound attacks of all types are increasing, but the increase in BEC and VEC is particularly worrisome, as socially-engineered threats continue to result in financial losses, data breaches, damage to brand reputation, and more. And with more organizations installing more third-party applications each and every day, the risk of attack via a side channel is rising rapidly.

Unfortunately, legacy email security tools are unprepared to stop these modern threats and security awareness training can only do so much to prevent employees from falling for an attack. To ensure complete protection against the full spectrum of attacks, from widespread spam to targeted BEC to third-party application abuse, organizations need an email security platform that can detect even minor deviations to identify anonymous activity and block attacks.

Implementing modern email security technology that pairs advanced behavioral science with risk-adaptive detection is the only surefire way to defend your organization against advanced inbound threats. **And to prevent the abuse of third-party applications, this same platform needs to monitor the email environment for high-risk configuration drifts—including new third-party applications, a change in permissions, or privilege escalations.**

It is only by protecting the whole email environment—inboxes and connected applications alike—that organizations can truly stay protected from the attacks of today and those of the future.



Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

More information is available at abnormalsecurity.com

**Interested in Protecting Your Email
from the Full Spectrum of Attacks?**

See Your ROI →

Get a Demo →