Abnormal

CISO Guide to Email Platform Attacks

New Vulnerabilities Impacting Cloud-Based Email

The Rising Threat of Email Platform Attacks

Cloud-based operations are increasingly popular among companies with distributed workforces. In fact, Gartner estimates that 70% of organizations have already made the move to cloud email and that 85% of organizations will be "cloud-first" by 2025. In many ways, this is a good thing, enabling increased productivity and better team collaboration. But these cloud platforms can also introduce new entry and exit points for attackers.

In fact, according to IBM's Cost of a Data Breach Report, nearly half (45%) of all data breaches in 2022 occurred in the cloud, making it a costly vulnerability for organizations across the board. Email in particular is vulnerable, as it serves as the main communications platform for all businesses, enabling your employees to speak with one another and with your vendors and to access connected applications like SharePoint. And perhaps most importantly, it serves as the key point of contact for all other applications—the one tool through which authentication occurs and password reset requests are sent.

All of this means that email is more likely than ever to be targeted, and no longer only by inbound threats, but also by a new type of attack that focuses on gaining access to the entire email platform.

Attackers will rely on cloud complexity, misconfigured security policies, and a lack of visibility into configuration changes to gain access and steal information. To combat these new email platform attacks, a new approach to cloud email security is needed.

45%

of data breaches occurred in the cloud.

11%

of companies are targeted by account takeover attempts each week.

Abnormal™

Types of Email Platform Attacks

Email platform attacks are far from a monolithic attack type. Much like the variations in business email compromise, these attacks involve the use of a wide spectrum of tactics that exploit user identities, applications, and mail tenants. At their core though, their goal is to gain access to the email platform, from which they can complete a number of nefarious activities. And they're successful because lax security configurations and a lack of visibility leave gaps often go undetected—except by threat actors themselves.

Here are a few types of email platform attacks today.

Account Takeover and MFA Bypass

When a threat group gets their hands on stolen user credentials, they often still need to contend with multi-factor authentication (MFA), particularly as more organizations have implemented this security best practice. One common method around this obstacle is a brute-force MFA attack, wherein an end user is inundated with push notification asking to confirm login until the user exhaustedly gives in and approves. Unfortunately, if that tactic fails, there are several to replace it, including the abuse of legacy authentication. If an organization has not disabled the use of legacy authentication on their cloud email platform, bad actors can sidestep MFA entirely by logging in through older mobile clients and mail protocols that do not support a second factor.

Malicious App Integration and Over-Permissioned Apps

App attacks come in a variety of flavors, and all of them are nefarious. Once a threat actor has gained access to an organization's cloud email platform, they can abuse API integration points or steal API keys to install malicious applications and give direct read/write access to a mail tenant. From there, they can impersonate compromised users, execute mass spam campaigns, or silently read and download sensitive messages. This same attack can be done in reverse as well, with users duped into downloading a seemingly legitimate application, which then steals user credentials and gains read/write access—acting instead as the entry point for attackers.

Privilege Escalation and Insider Threats

Privileged accounts are a playground for both external threat actors and malicious insiders. In the case of external attackers, privileged accounts like that of executives are often a target. If an attacker commandeers a privileged account, that account can then be used to compromise additional accounts across the email platform and change critical configurations–such as abusing mail forwarding rules to silently exfiltrate corporate communications, lock out all other administrators, and effectively hold systems hostage.

Impact of Email Platform Attacks

According to IBM's 2022 Cost of a Data Breach report, cloud misconfigurations accounted for 15% of all breaches. In real dollars, this translates to $4.14M in losses. While the costs alone are staggering, there is an additional disturbing layer, as breaches caused by cloud misconfiguration took an average of 183 days to identify and then another 61 days to contain.

As most attackers exfiltrate data within five hours of gaining access, spending three-quarters of a year simply uncovering and responding to a breach is less of a remediation effort and more supremely-delayed damage control.

Beyond data exfiltration, however, is the risk of reputational damage as some email platform attacks do not result in a data breach but rather target consumers. In one example discovered by Microsoft, a nation-state actor compromised a series of mail tenants through compromising user accounts, bypassing MFA, and then installing malicious applications in the environment, with the ultimate goal being the execution of a massive spam campaign. Consumers were sent emails that appeared to come from legitimate brands, claiming the recipient had won a prize. In actuality, the recipients would enter their personal information and be enrolled in a paid monthly subscription to nothing.

In another example that used a malicious third-party application, a major media organization fell victim to a breach that began two years before it was ultimately discovered. Attackers installed an application into the organization's Azure environment, which then continually reported daily logs and searches back to the threat group's server. As this application had direct access to the Microsoft 365 tenant without needing to bypass MFA or gain admin access, it went undetected by traditional solutions that were not monitoring for app permissions or cataloging trusted applications across the enterprise.

And unfortunately, it is not only large corporations that are being targeted. These attacks can impact organizations of all sizes and all industries, as threat actors often look for the points of least resistance in their schemes.

Why Email Platform Attacks are Successful

Stopping email platform attacks takes a proactive approach to cloud email security. Legacy solutions often lack visibility into the activity occurring across a cloud email platform's users, applications, and tenants—and even those that do provide that insight lack the ability to contextualize and correlate activity to identify risks.

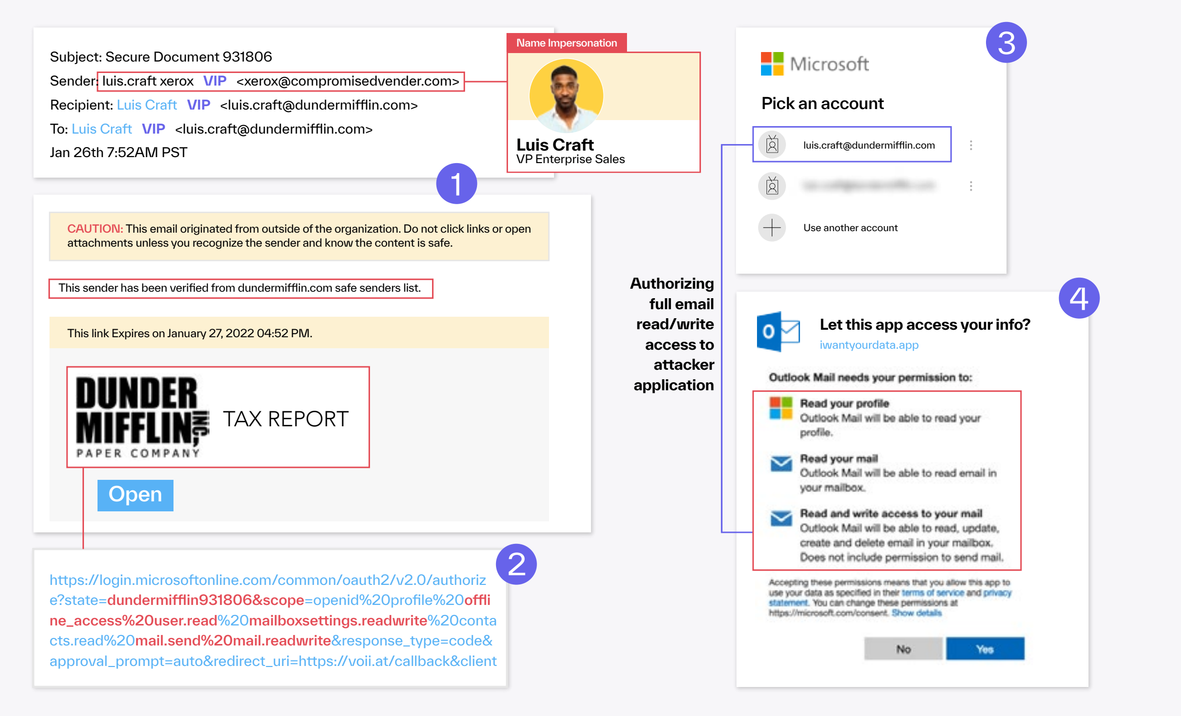
Aside from solution gaps, IT and security organizational structure plays a significant part in allowing cloud email platform attacks to flourish. In many organizations, security either shares responsibility or is not responsible for securing SaaS applications. In fact, in a 2022 Cloud Security Alliance survey, 41% of respondents indicated that the application owner was primarily responsible for the security of the application.

While it is imperative to ensure every member of an organization practices good security hygiene if they want to install new technologies, coupling that 41% with the reported lack of visibility security teams have into application permission and configuration changes means an attacker may not need to outfox a security professional at all. When the average organization has deployed 254 SaaS applications, they only need to wait for someone in legal, marketing, sales, or another department to misconfigure a critical application. With 40% of organizations providing those departments access to app security settings, this access could lead to devastating losses. And this is only the application side—saying nothing about those attacks that target user permissions or tenant changes.

A Real-World Attack Using Third-Party Applications

You don't necessarily have to take our word for it either. **Let's take a look at a real-world example and see why a legacy cloud email security tool may fall short.**

In the example illustrated in the diagram below, the attack begins with an email sent from what appears to be a trusted vendor. The email address and domain match a known third-party sender, so the email bypasses legacy solutions and the recipient opens it. They find a link to what again, appears to be a legitimate third-party Microsoft authentication page, prompting the user to enter their Microsoft credentials and grant access to an attacker-owned application.



Subject: Secure Document 931806
Sender: luis.craft xerox VIP <xerox@compromisedvender.com>
Recipient: Luis Craft VIP <luis.craft@dundermifflin.com>
To: Luis Craft VIP <luis.craft@dundermifflin.com>
Jan 26th 7:52AM PST

Name Impersonation
Luis Craft
VP Enterprise Sales

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

This sender has been verified from dundermifflin.com safe senders list.

This link Expires on January 27, 2022 04:52 PM.

DUNDER MIFFLIN INC. PAPER COMPANY TAX REPORT

https://login.microsoftonline.com/common/oauth2/v2.0/authorize?state=dundermifflin931806&scope=openid%20profile%20offline_access%20user.read%20mailboxsettings.readwrite%20contacts.read%20mail.send%20mail.readwrite&response_type=code&approval_prompt=auto&redirect_uri=https://voii.at/callback&client

Microsoft
Pick an account
luis.craft@dundermifflin.com
Use another account

Authorizing full email read/write access to attacker application

Let this app access your info?
iwantyourdata.app

Outlook Mail needs your permission to:

Read your profile
Outlook Mail will be able to read your profile.

Read your mail
Outlook Mail will be able to read email in your mailbox.

Read and write access to your mail
Outlook Mail will be able to read, update, create and delete email in your mailbox. Does not include permission to send mail.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://microsoft.com/consent. Show details

Once the malicious app is integrated into the email platform, the threat actor gains access to the recipient's mailbox and can launch additional attacks. Not only does the attacker have access to read the profile and email, but he can also send additional emails, use that access to move into other applications, or add additional third-party applications to the tenant—providing the ability to do just about anything he chooses across the organization.

Could you spot the ways this evades a traditional email security solution?

The trusted sender—possibly a compromised vendor account—is already part of the recipient's safelist and does not raise any red flags for a secure email gateway to review. While there is a link in the email, it is a legitimate Microsoft authentication page. It only masks the malicious application that is to be installed once the recipient authenticates.

And, email security solutions often start and end with their namesake—email security. They do not extend across the cloud email platform and do not provide security teams with visibility into installed third-party applications and their corresponding permissions. Thus, once this inbound attack bypasses the solution, there is often limited ability for legacy tools to highlight anomalous activity—and if those tools can it typically is not contextualized in a singular location in a way that truly aids investigation.

How to Stop Email Platform Attacks

In order to detect and prevent email platform attacks, it's crucial that your organization implement an effective security posture management system that provides insight into configuration changes across your environment. At Abnormal, we've reimagined how security posture should be handled, integrating our new Security Posture Management product directly with our Cloud Email Security platform.

This provides increased visibility across the email ecosystem and expands what true cloud email security should be. Using Knowledge Bases that understand your people, vendors, applications, and tenants, Security Posture Management provides you insights into when changes have occurred across your environment so you can take the appropriate downstream action.

A modern solution to cloud email security that protects against these email platform attacks includes:

Enhanced Email Attack Detection

A solution that uses behavioral AI to learn your organization's email platform usage and communication patterns better protects the front door—as more than 90% of all attacks still involve phishing and social engineering in some capacity. This solution must also help you gain visibility into anomalous user activity indicating account takeovers or notable configuration changes that may indicate a bad actor is in your environment.

Increased Visibility Into Configurations In Your Posture

An easily searchable inventory of users, tenants, vendors, and third-party applications. It automatically surfaces potential misconfigurations, as well as configuration changes that could impact your overall security posture across the cloud email environment.

Reduced Manual Efforts Managing Configuration Changes

A solution that eliminates cumbersome manual processes used to record critical email platform configurations, user identities and privileges, and app integrations and permission. This record should be tied to an acknowledgment workflow to improve security efficiency and cross-team visibility into which items are being addressed.

Conclusion

There is no doubt that threat actors are becoming more sophisticated every day. Email platform attacks continue to rise because cloud configurations have become exceedingly difficult for security teams to track and manage. By infiltrating unguarded entry points within a cloud email platform, attackers can access either an individual account or the entire email platform, resulting in costly breaches. And because they've been successful up to now, these attacks are only going to increase in frequency and severity.

Stopping these attacks requires increased platform visibility through the implementation of an effective security posture management system. By doing so, you can ensure that your security team knows when changes occur across your environment, and have the information they need to proactively stop potential attack entry points—before they become the next way for threat actors to target you.

Abnormal

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Interested in stopping email platform attacks?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@abnormalsec

v1.0/JAN. 2023