Abnormal

CISO Guide to Collaboration App Attacks

How to Protect Your Communications Applications

176%

increase in usage of collaboration apps in 2020.

Absolute

82%

of all organizations use more than 6 collaboration tools.

ESG

69%

of security leaders are somewhat or extremely concerned about multi-channel attacks that utilize collaboration tools.

ESG

The Rising Risk of Collaboration App Attacks

Slack. Microsoft Teams. Zoom. Jira. Asana. Confluence. The list of collaboration applications has never been more extensive. As organizations have moved to remote and hybrid work, with employees spread across the globe, there has been an increased need for communications applications that will let them continue to do their best work—no matter where they are.

There is no denying that these tools make it easier for employees to communicate, share files, and manage projects. But what is good for business is oftentimes also good for cybercrime.

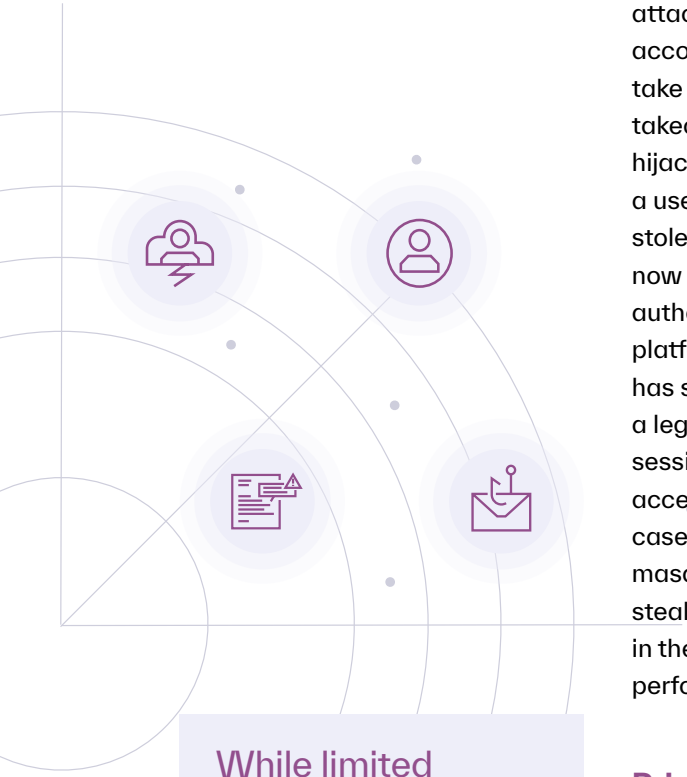
The sheer number of collaboration tools available today means that employees are shifting away from email as the only form of communication and toward these many other tools—most of which do not have the same level of security as the Microsoft or Google email environment. As a result, by targeting one of these applications, attackers can evade traditional email security controls and extend their credential phishing, social engineering, and malware attacks to target employees where they are.

And unfortunately, where employees have been trained to be suspicious of emails that make unusual requests or ask them to send money, this is not yet the case for these more casual communications applications—making them an easy next target for cybercriminals.

As more organizations implement advanced email protection, it is only a matter of time before threat actors turn to other collaboration tools to run their scams. And in some instances, **they already have.** Traditional email security solutions are designed only to protect against email threats, but as cybercriminals move on, so does the need for cybersecurity. Without a new approach to email security—one that also protects these email-like communications applications—organizations will remain susceptible to attack.

Types of Collaboration App Attacks

Considering the variety of uses for collaboration apps, it only makes sense that there are a variety of attack types, which may change slightly depending on the collaboration app targeted.



While limited visibility into these applications and the increasing creativity of attackers are the ingredients for disaster, understanding these attack types is the first step in stopping them.

Account Compromise and Session Hijacking

Oftentimes, the first step in executing a collaboration app attack is compromising the account. This compromise can take one of two forms: an account takeover attack or a session hijacking attempt. In the former, a user has had their credentials stolen, and a threat actor is now using that account to authenticate into a collaboration platform. In the latter, the attacker has stolen the session tokens for a legitimate authentication session, giving them immediate access to an application. In both cases, the attacker can then masquerade as the user, stealing sensitive information in the account, or using it to perform additional attacks.

Privilege Abuse

Configuration risk is the final threat to these collaboration platforms. Attackers with administrative rights can access private channels, change authentication methods, or export data to other applications. Alternatively, if the organization has not practiced good data hygiene or integrated sensitive data from additional applications into their tenant, attackers can quickly exfiltrate this data.

Phishing

Phishing and social engineering are both similar and starkly different from the attacks you'd expect in the email inbox. In terms of similarities, users inherently trust messaging platforms like Slack and the chat capabilities in Zoom. Threat actors can send malicious content to prey on this trust, similar to any email phishing campaign, to encourage the victim to input credentials into a variety of sites. These attacks can occur in multiple ways, either by compromising or impersonating an internal user or an external partner via a feature like Slack Connect.

Social Engineering

Business email compromise has been the most financially-damaging attack for the past eight years, and the social engineering tactics it relies on can be even more insidious on collaboration apps. For example, Microsoft Teams channels specifically for IT access requests can be abused to give attackers admin permissions, or they can be used to bypass MFA requests for other applications. Alternatively, Zoom can be used in deepfake phishing attacks where attackers use the voice and visage of an executive to convince an employee to take action.

The Impact of Collaborative App Attacks

89%

of organizations report having seen at least one advanced attack targeting their collaboration platforms.

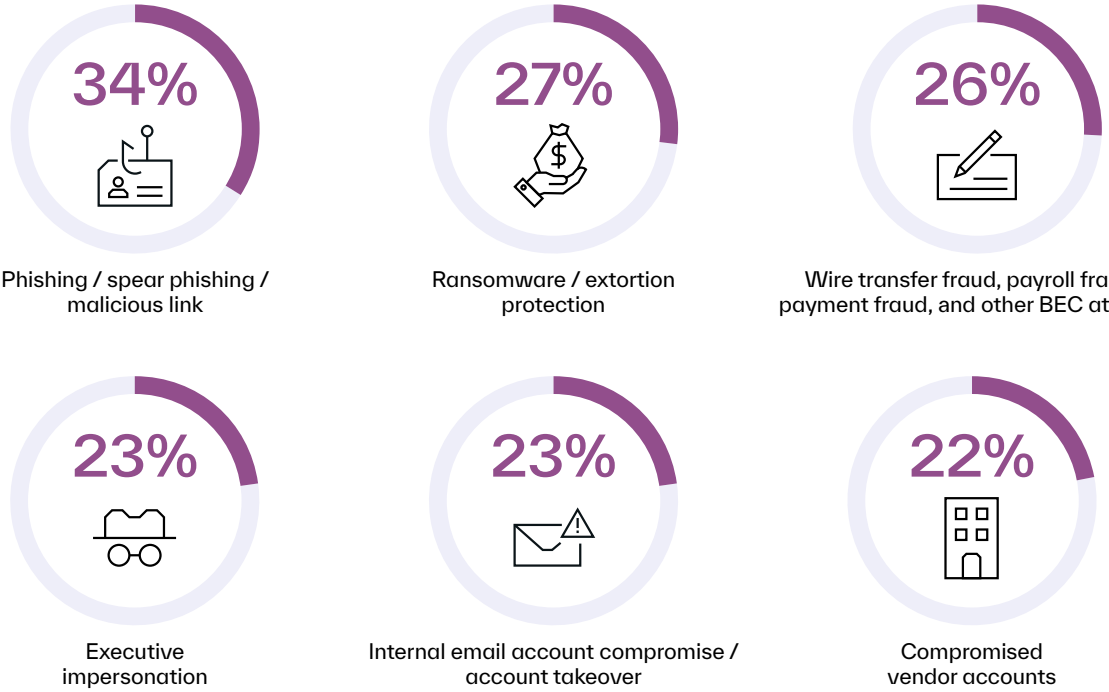
ESG

Recent research conducted by analyst firm, Enterprise Strategy Group (ESG), found that 89% of organizations report having seen at least one advanced attack targeting their collaboration platforms.

Couple that 89% with the knowledge that over half of all respondents (52%) deal with weekly or daily multi-channel attacks targeting both email and collaboration apps, and it paints a grimmer portrait of the collaboration application threat landscape.

Even with such a high incidence of collaboration app abuse reported, many of these attacks have not been publicized, making it difficult to truly know the impact. But in the attacks that have been made public, there have been major consequences. For example, when the CCO of Binance was impersonated on Zoom via deepfake, the organization saw immediate customer concerns. And when stolen credentials were used to gain access to Slack at Rockstar Games, portions of their flagship Grand Theft Auto game leaked online.

Types of Threats Penetrating Communication and Collaboration Security Controls



ESG Survey, The Freedom to Communicate and Collaborate, 2023.

Why Collaboration App Attacks Are Successful

An interesting statistic from ESG's research is that roughly 60% of organizations feel the native security controls in collaboration apps are enough and that the security team has excellent visibility into these channels.

But with 89% of those same respondents experiencing attacks on their collaboration apps, there is a discrepancy between industry sentiment and the threatening reality. This discrepancy highlights one of the key reasons these attacks are successful: human trust.

Just as security professionals are wont to trust native tools until proven otherwise, end users on collaboration apps are more likely to trust a message coming from what they assume is a coworker or partner.

Employees receive constant education on the risks of email phishing and social engineering so are already wary of unusual messages hitting their inbox. But security awareness training has not yet extended to other applications, so employees may not have the same suspicions when it comes to a Slack message or a Teams invite. This allows attackers to exploit employee trust to complete their attack.

The Attack on Rockstar Games

What Happened at Rockstar Games?

The attack began with a purchase, likely on the Dark Web. The threat landscape is less of a disjointed tapestry of actors and more of an inverse cybersecurity industry, with threat actors selling everything from stolen cookies to purpose-built solutions for deploying ransomware. In this case, the attackers bought stolen Slack session cookies for only $10.

With those cookies, attackers gained access to Rockstar Games' corporate Slack channels *as the user whose cookies had been stolen.* The attackers began impersonating this user by hijacking a single session, but they did not (initially) have full access to that user's account.

To gain that access, the attackers messaged IT support, as the impersonated user. They explained that they had lost their second-factor device, and convinced IT to send multi-factor authentication tokens to them—which IT did. As an aside, IT should not be faulted in this case, as by all accounts, this was a legitimate user requesting IT help.

After this bit of social engineering, the attackers had free reign to dive deeper into Rockstar Games' network, eventually stealing video game source code that leaked across the Internet—all from a single Slack session.

How to Protect Your Collaboration Apps

As most documented collaboration app attacks have only occurred in the last two years, this is a relatively new segment of the threat landscape. That said, it's one that is accelerating quickly as the adoption of these platforms, the shift towards remote work, and the always-on mentality of global employees shows no signs of slowing.

Native security tools simply aren't enough to stop modern and multi-channel attacks, and no organization wants to implement point solutions for every single application. To effectively protect collaboration platforms, organizations should look for solutions that contain the following elements and capabilities:

Behavorial AI Approach

The solution should use a fundamentally different approach that leverages behavioral data science and AI to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop users that appear suspicious, and include the ability to detect whether a message sent via collaboration apps contains malicious links or content.

API Architecture and Integrations

A solution that connects to Microsoft 365 and Google Workspace via an API and in doing so, provides access to the signals and data needed to detect suspicious activity not only across these email platforms but also across email-like communications applications. This includes unusual geolocations, dangerous IP addresses, changes in rules, unusual device logins, and more. Advanced solutions should ingest and analyze signals from not only collaboration apps like Slack and Zoom but also from authentication platforms like Okta and XDR solutions like CrowdStrike, to understand identity and cross-platform activity and detect multi-channel attacks.

Secure Privileges and User Configurations

One errant over-privileged user can spell disaster, whether that user is an outside actor commandeering a compromised account or a malicious insider attempting to gain unauthorized control of a platform. Beyond messaging and authentication activity, an effective solution must also surface high-impact changes to user privileges. As security teams often lack visibility into these changes, any surfaced event must include contextual insights into why this change matters and what can be done to remediate the issue.

Without each of these capabilities, collaboration and communications applications remain open to attack, and threat actors will turn to them as they look to expand their cybercrime operations.

Conclusion

The increased usage of applications like Slack, Microsoft Teams, and Zoom showcases how organizations are shifting operations, but also highlights the need for more security protocols to protect these platforms. By infiltrating email-like applications and exploiting human trust, threat actors are finding new vulnerabilities allowing them to teal money and gain access to sensitive data.

Stopping these attacks requires a solution that uses a fundamentally different approach to security. By understanding known behavior across email and email-like applications, modern security solutions can detect attacks on collaboration applications and stop them before they can trick employees and cause damage to your organization.

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 Collaboration Applications?

See Your ROI → Get a Demo →