Adding collaboration app security for Microsoft 365 to your email security stack

State of Microsoft 365 collaboration apps

As organizations across the world have adopted Microsoft 365, collaboration applications in Microsoft 365 have become an integral part of everyday operations, communications and productivity.

With Microsoft Teams being used by more than one million organizations and the number of daily active users growing more than 1,000% between 2019 and 2023, the adoption of Microsoft 365 collaboration applications like Teams, OneDrive and SharePoint is growing rapidly and showing no signs of slowing down.

Challenges

Cyberattackers are focusing more on critical Microsoft 365 applications, using advanced methods and exploiting weaknesses to launch attacks. According to Perception Point, collaboration channels are more prone to advanced attacks — almost 10 times more than email. In 2023, 40% of organizations using Microsoft 365 encountered at least one attack via its collaboration tools.

Phishing and impersonation attempts shared via Teams or via embedded links within files, are common tactics that account for 15% of Microsoft 365 attacks. Threat actors craft convincing messages to trick users into taking harmful actions or divulging credentials that are then used to access sensitive data stored in Microsoft 365 apps.

Unlike in email, malware distribution is the most prevalent accounting for 65% of attacks, with attackers exploiting vulnerabilities in file-sharing features or injecting malicious links into collaboration channels to infect users' devices and compromise organizational networks.

Moreover, the integration and interconnectedness of Microsoft 365 apps provide attackers with avenues to conduct lateral movement within organizations' environments, facilitating data exfiltration, espionage or disruption of critical operations. As a result, organizations must prioritize direct cybersecurity measures for these apps to mitigate the risks posed by these evolving cyberthreats targeting Microsoft 365 apps.

Documented threats examples

TeamsPhisher in Teams

Attack method: Exploiting the platform's trust and familiarity, attackers typically impersonate trusted contacts or IT support within Microsoft Teams, sending phishing messages with malicious links or attachments.

Execution: Creating a sense of urgency or curiosity, attackers prompt users to click on links or provide login credentials, stealing user credentials and leading to unauthorized access to Teams accounts and sensitive data or further exploitation within the organization.

Impact: Successful attacks cause data breaches, account compromise and potential dissemination of malware or further phishing attempts.

Malicious links in OneDrive

Attack method: Attackers send phishing emails containing links to malicious websites hosted on OneDrive. These websites may mimic legitimate login pages or prompt users to download fake documents.

Execution: By masquerading as legitimate notifications or alerts, attackers trick users into clicking on these links, leading to credential theft, malware infection or unauthorized access to OneDrive files.

Impact: Compromised credentials can be used to access sensitive data stored in OneDrive, facilitating data theft, insider impersonation, espionage or further infiltration into the organization's network.

File upload exploits in SharePoint

Attack method: Attackers exploit vulnerabilities in the platform's file upload functionality to upload malicious files containing malware or scripts.

Execution: By uploading files containing malware, scripts or other malicious content to SharePoint sites, the malicious files can spread within an organization's SharePoint environment, potentially infecting other users' devices or compromising the integrity of SharePoint sites.

Impact: The impact of file upload exploits can be severe, leading to malware infections, data breaches or system compromise. Additionally, compromised SharePoint sites may become platforms for further attacks, enabling attackers to distribute malware, steal data or launch additional cyberthreats within the organization.

The solution

Secure critical Microsoft 365 collaboration resources with the most effective advanced threat prevention solution on the market. Replace or augment the limited security capabilities included in Microsoft deployments and / or in Microsoft Defender for Office 365. Acronis' multilayered security protects your organization from signature-based (known) and advanced (unknown) attacks. Acronis performs dynamic scans on all traffic to detect malicious content, and when such content is identified, it alerts teams and prevents the threat from reaching end users. Acronis achieves this by continuously scanning every file and URL for various content-related threats, including ransomware and malware, malicious URLs embedded in files, and advanced attacks like APTs and zero-day exploits.

Additionally, our managed incident response service grants you direct access to cyber analysts who are available 24/7. These experts can assist you in further investigating incidents, offering clarification, and, if necessary, remedying incidents promptly.

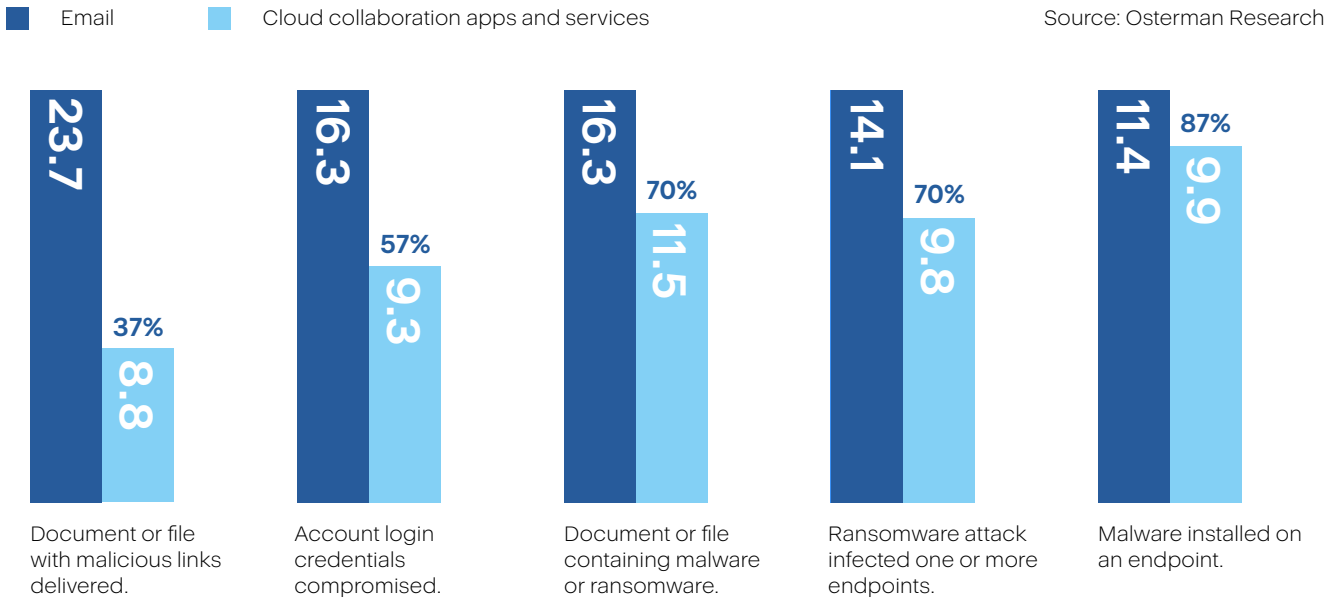
Conjunction with email

The integration between email and collaboration apps facilitates the spread and escalation of cyberthreats within organizations. Attackers can move laterally between these interconnected systems, exploiting weaknesses in security controls or user behaviors to achieve their objectives.

Email serves as a primary communication channel used for sharing files, coordinating tasks and collaborating with colleagues. However, email is also a common vector for cyberthreats, including phishing, malware distribution and social engineering attacks. Not surprisingly, over 68% of cyber breaches involve human error, according to the "2024 Data Breach Investigations Report" by Verizon.

Once compromised, attackers can leverage stolen credentials or exploit vulnerabilities within email platforms to launch further attacks across collaboration apps such as Teams, OneDrive and SharePoint. Successful email incidents can extend into more severe attacks through collaboration apps, and data now show the synchronicity of attacks at scale. Successful incidents against collaboration apps are approaching the baseline in email, as shown in the graph below.

Successful incidents against cloud collaboration apps (normalized to email)



An example of a common cross-channel attack

Stolen credentials obtained through a phishing attack via email can be used to access SharePoint sites or OneDrive accounts where sensitive data may be stored and impersonation attacks can go unchecked.

Similarly, malware distributed through via attachments can propagate to collaboration platforms, infecting shared files in OneDrive or spreading within Teams channels.

By addressing vulnerabilities in both email and collaboration apps, organizations can mitigate the risks associated with cyberthreats and safeguard their digital assets effectively.

Footnotes

https://www.verizon.com/business/resources/reports/dbir/#DBIR2024NR
https://ostermanresearch.com/2022/11/25/rise-cyberthreats-perceptionpoint/

Acronis

Learn more at
www.acronis.com