Incident Responders Explore Microsoft 365 Attacks in the Wild

By Kelly Sheridan

Published: 2021-08-05 · Archived: 2026-04-05 15:48:04 UTC

IB Photography via Adobe Stock

BLACK HAT 2021 – Microsoft 365 is a hot target for cybercriminals, who constantly seek new ways to bypass its safeguards to access corporate data. And as defenders step up their game, attackers do the same.

"This past year has proved the point that nation-state-backed threat actors are increasingly investing time and money to develop novel ways to access data in Microsoft 365," said Josh Madeley, manager of professional services at Mandiant, in a briefing entitled "Cloud with a Chance of APT: Novel Microsoft 365 Attacks in the Wild" during this year's Black Hat USA.

These attackers are especially interested in Microsoft 365 because it's where more and more organizations store their data and collaborate, Madeley continued. Applications such as email, SharePoint, OneDrive, and Power BI can hold a wealth of information invaluable to attackers.

"If you're an espionage-motivated threat actor, Microsoft 365 is the holy grail," he said.

In the talk, Madeley and co-presenter Doug Bienstock, incident response manager at Mandiant, walked through lessons learned from large-scale espionage campaigns they've observed over the past year. Techniques they saw helped attackers disable security features like auditing and logging, automate data theft with old tactics, and abuse enterprise applications with new ones. They also maintained their access by abusing SAML and Active Directory Federation Services.

Madeley kicked off the talk with methods for evading detection. Attackers aren't interested in modifying data, he said. They want to steal the data, review it, and understand it. There are stealthy ways to do this, but attackers want to improve on their tactics and make it harder for defenders to catch them – "especially if they want to perpetrate data theft over years," he said.

One way they do this is by disabling security features. All domain admins have access to the audit logs in Microsoft 365, though organizations that pay for an E5 subscription have access to advanced auditing. This comes with MailItemsAccessed, a feature that records any interactions with mail item objects within a 24-hour period, after which it's throttled.

It's a problematic feature for attackers looking to steal from corporate mailboxes, Madeley noted. They needed to find a way around it.

"Fortunately, Microsoft handed it to them in the Set-MailboxAuditBypassAssociation cmdlet," he continued. This prevents the logging of mailbox actions for specific users. When configured, any mailbox owner actions made by specified users who have the bypass configuration aren't going to be logged. Delegate actions performed by specified users on other target mailboxes are not logged, and certain admin actions are also not going to be logged, Madeley explained.

"You'd be well-served to monitor for the execution of this cmdlet in your tenant," he said of Set-MailboxAuditBypassAssociation. If an organization is monitoring for data theft, it may miss malicious activity if an attacker's target inbox isn't being logged.

A more efficient way to bypass logging is to downgrade critical users' licenses from E5 to E3, Madeley said. This disables MailItemsAccessed logging without affecting any of the features most people will use on a daily basis.

"These are really simple techniques, once you give admin access to a tenant, to make these changes to enable long term data theft," he added.

Mailbox Folder Permission Abuse

Another technique discussed was the abuse of mailbox folder permissions, which act as an alternative to mailbox delegations. Within a mailbox, an owner, admin, or account with full access permissions can grant permissions to other users that allow them to access specific folders within a mailbox. There are many legitimate use cases for this: sharing calendars, having team mailboxes, or allowing admin assistants to access particular folders.

"Just like administrators, attackers who have acquired sufficient permissions to a mailbox or a tenant can modify these permissions to allow them to access the folder contents," Madeley said. It's an older technique first documented by Black Hills Security in 2017 but is still effective.

The incident response team recently saw an APT actor lose access to multiple environments using a sophisticated means of targeting mailboxes, only to fall back on this method of abusing mailbox folder permissions.

"What was even more fascinating is, when they fell back on this method, there were no modifications made to the environment to enable it during the time of our investigation, which meant that those changes had been made a long time before," he noted.

Attackers will ultimately be after roles with ReadItems permissions, as this grants access to read mail items in a specific folder. There are several roles with this permission: Author, Editor, NonEditingAuthor, Owner, PublishingEditor, PublishingAuthor, and Reviewer. Madeley said that Reviewer, specifically, is the one his team has seen attackers use.

In addition to users within the tenant, there are two special users: an anonymous user, or any external unauthenticated user, and the default, or "everyone" user. The latter includes any internal and authenticated users. By default the access for both user types is set to None.

However, an attacker can take advantage. Madeley has seen attackers assign a default user to the Reviewer role, which would allow any authenticated user access to the mailbox folder. Permissions don't cascade down from "child" to "parent" for existing folders, but newly created folders will inherit the permission. This can be "trivially done" using the Set-MailboxFolderPermission cmdlet, he noted.

The attacker will still need to maintain some level of access through a valid account; however, with this modification, they don't need to maintain access to a specific account they want to target on a daily or weekly basis. Instead, they can use one compromised account to access 10 mailboxes with modified folder permissions.

About the Author

Former Senior Editor, Dark Reading

Kelly Sheridan was formerly a Staff Editor at Dark Reading, where she focused on cybersecurity news and analysis. She is a business technology journalist who previously reported for InformationWeek, where she covered Microsoft, and Insurance & Technology, where she covered financial services. Sheridan earned her BA in English at Villanova University. You can follow her on Twitter @kellymsheridan.
