Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452

fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html

Breadcrumb

Threat Research

Mike Burns, Matthew McWhirt, Douglas Bienstock, Nick Bennett, Juraj Sucik

Jan 19, 2021

5 mins read

TTPs

Uncategorized Groups (UNC Groups)

Threat Research

UPDATE (May 2022): We have merged UNC2452 with APT29. The UNC2452 activity described in this post and report is now attributed to APT29.

UPDATE (Oct. 28, 2021): Mandiant has recently observed targeted threat actors using EWS impersonation (via the ApplicationImpersonation role) to maintain persistent access to mailboxes in victim environments. Once the threat actor has access to this role, its abuse is hard to detect and provides the threat actor control over every mailbox in a victim tenant. Mandiant has also observed targeted threat actors abusing the trust relationship between Cloud Service Provider (CSP) organizations and their customers to laterally move from service providers to their downstream customers and gain administrator privileges in the target tenants. The blog post, white paper, and Azure AD Investigator tool have been updated to reflect these findings.

UPDATE (Mar. 18): Mandiant recently observed targeted threat actors modifying mailbox folder permissions of user mailboxes to maintain persistent access to the targeted users' email messages. This stealthy technique is not usually monitored by defenders and provides threat actors a way to access the desired email messages using any compromised credentials. The white paper, blog post and Azure AD Investigator tool have been updated to reflect these findings. Mandiant would like to thank the members of Microsoft's Detection and Response Team (DART) for their collaboration on this research.

In December 2020, FireEye uncovered and publicly disclosed a widespread attacker campaign that is being tracked as UNC2452. In some, but not all, of the intrusions associated with this campaign where Mandiant has visibility, the attacker used their access to on-premises networks to gain unauthorized access to the victim's Microsoft 365 environment.

Goals and Objectives

Methodologies that UNC2452 and other threat actors have used to move laterally from on-premises networks to the Microsoft 365 cloud have been detailed in our white paper, *Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452*. The paper also discusses how organizations can proactively harden their environments and remediate environments where similar techniques have been observed.

Mandiant is releasing an auditing script, Azure AD Investigator, through its GitHub repository that organizations can use to check their Microsoft 365 tenants for indicators of some of the techniques used by UNC2452. The script will alert administrators and security practitioners to artifacts that may require further review to determine if they are truly malicious or part of legitimate activity. Many of the attacker techniques detailed in the white paper are dual-use in nature—they can be used by threat actors but also by legitimate tools. Therefore, a detailed review for specific configuration parameters may be warranted, including correlating and verifying that configurations are aligned with authorized and expected activities.

Attacker Tactics, Techniques and Procedures (TTPs)

Mandiant has observed UNC2452 and other threat actors moving laterally to the Microsoft 365 cloud using a combination of five primary techniques:

1. Steal the Active Directory Federation Services (AD FS) token-signing certificate and use it to forge tokens for arbitrary users (sometimes described as Golden SAML). This would allow the attacker to authenticate into a federated resource provider (such as Microsoft 365) as any user, without the need for that user's password or their corresponding multi-factor authentication (MFA) mechanism.
2. Modify or add trusted domains in Azure AD to add a new federated Identity Provider (IdP) that the attacker controls. This would allow the attacker to forge tokens for arbitrary users and has been described as an Azure AD backdoor.
3. Compromise the credentials of on-premises user accounts that are synchronized to Microsoft 365 that have high privileged directory roles, such as Global Administrator or Application Administrator.
4. Backdoor an existing Microsoft 365 application by adding a new application or service principal credential in order to use the legitimate permissions assigned to the application, such as the ability to read email, send email as an arbitrary user, access user calendars, etc.
5. Modify the permissions of folders in a victim mailbox (such as the inbox) to make its contents readable by any other user in the victim's Microsoft 365 environment.
6. Use EWS Impersonation to impersonate any mailbox owner in the Microsoft 365 tenant and bulk collect mail items.
7. Target and compromise Cloud Service Providers (CSPs) that have permissions to administer customer tenants of organizations that UNC2452 is targeting, and abuse the access granted to the CSP to perform post-compromise activities against the target organization.

Read the white paper for a detailed overview of each technique, including practical remediation and hardening strategies, and check out our auditing script, Azure AD Investigator.

Detections

FireEye Helix Detection	MITRE Technique	Detection Logic
MICROSOFT AZURE ACTIVE DIRECTORY [Risky Sign-In]	T1078.004	Alert on suspicious logon activity as detected by Azure Identity Protection

OFFICE 365 [Federated Domain Set]	T1550	Alert on new domain federation in Office 365
OFFICE 365 [Modified Domain Federation Settings]	T1550	Alert of modification to domain federations settings in Office 365
OFFICE 365 [User Added Credentials to Service Principal]	T1098.011	Alert on addition of certificates or passwords added to Service Principals
OFFICE 365 ANALYTICS [Abnormal Logon]	T1078.004	Alert on suspicious login activity based on heuristics
WINDOWS METHODOLOGY [ADFS Dump]	TA0006 T1552 T1552.004 T1199	Alert on activity access requests for the AD FS Distributed Key Manager (DKM) container in Active Directory
OFFICE 365 [Mailbox Folder Permission Change – Inbox and Top Of Information Store]	T1098.002	Alert on suspicious modifications of mailbox folder permissions for the inbox or top of information store.