Office 365

AUDIT LOG

Artifact Reference Guide

Created by the Microsoft Incident Response Team

Administrative Impact

Exchange and SharePoint actions which require administrative privilege to perform. These actions can extend the Threat Actors access to services in Office 365

- Remove-MailboxPermission
- Add-RecipientPermission
- Remove-RecipientPermission
- New-ManagementRoleAssignment
- Remove ManagementRoleAssignment
- SiteCollectionAdminAdded
- SiteCollectionAdminRemoved
- SharingPolicyChanged

Email manipulation

Defence evasion and social engineering

- Soft Delete
- Hard Delete
- TIMailData
- Set-InboxRule
- New-InboxRule
- Remove-InboxRule
- Enable-InboxRule
- UpdateInboxRules
- Create
- Send
- SendOnBehalf
- SendAs
- MoveToDeletedItems

Reconnaissance

Discovery actions

- Mailbox Login
- SearchQueryInitiatedExchange
- Page Viewed
- SearchQueryPerformed
- SearchQueryInitiatedSharePoint

Mailbox Actions

Actions performed on a compromised mailbox

- Set-Mailbox
- AddFolderPermissions
- ModifyFolderPermissions
- Set-MailboxJunkEmailConfiguration

Data Collection

Actions which allow data exfiltration

- MailItemsAccessed
- Update
- FileDownloaded
- FileAccessed
- SharingInvitationCreated
- SharingSet
- FileSyncDownloadedFull
- SearchExported
- SearchExportDownloaded

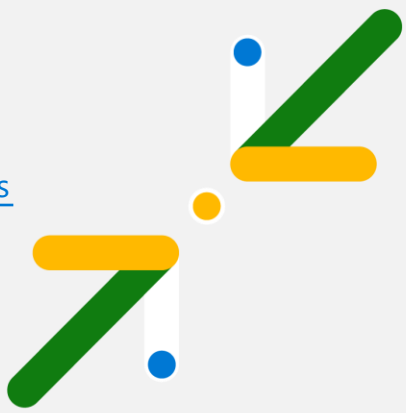
Impact

Actions which are destructive in nature

- SiteDeleted
- FileRecycled
- FolderRecycled
- FolderDeleted
- FileDeleted
- FileDeletedFirstStageRecycleBin
- FileDeletedSecondStageRecycleBin
- FolderDeletedFirstStageRecycleBin
- FolderDeletedSecondStageRecycleBin
- FileMalwareDetected

Interfaces

→ New Audit Search
→ Defender for Cloud Apps
→ Azure Sentinel



Microsoft Security

→ Good UAL Hunting → Audit log activities

Microsoft Entra ID

Artifact Reference Guide

Created by the Microsoft Incident Response Team

Login Events

Sign-in data and associated events

- UserLoggedIn
- UserLoginFailed
- Fraud reported – no action taken
- Fraud reported – user is blocked for MFA
- Suspicious activity reported

Applications

Privilege escalation and data access

- Consent to application
- Update application - certificates and secrets management
- Add owner to application
- Add owner to service principal
- Add service principal
- Add application
- Update application
- Update service principal

Devices

Modification of device objects

- Add registered owner to device
- Add registered users to device
- Add device

Impact

Actions which are destructive in nature

- Remove member from role
- Remove eligible member from role
- Update conditional access policy
- Delete conditional access policy
- User deleted security info
- Admin deleted security info
- Delete application
- Set accidental deletion threshold
- Bulk delete users - finished (bulk)

User Activity

Modification of user objects

- Add user
- Change user password
- User registered security info
- User registered all required security info
- Admin registered security info
- Download users – finished (bulk)
- Download service principals – finished (bulk)
- User started password reset
- Enable account

Identity

Changes to the identity plane

- Set federation settings on domain
- Add unverified domain
- Verified domain
- Set domain authentication
- Update domain
- Verify domain

Administration

Changes to role assignments

- Add eligible member to role
- Add member to role
- Set company information
- Add conditional access policy
- Elevate Access

Interfaces

- → Entra ID Audit Log
- → Entra ID Sign-in Log
- → Azure Sentinel
- → Unified Audit Log

Microsoft Security

→ Good UAL Hunting → Audit log activities