Behavioral Detection of Mailbox Data and Log Deletion for Anti-Forensics, Detection Strategy DET0266

Archived: 2026-04-05 16:51:30 UTC

AN0737

Detects mailbox manipulation or deletion via PowerShell (e.g., Remove-MailboxExportRequest), file deletion from Outlook data stores (Unistore.db), or tampering with quarantined mail logs.

Log Sources

Mutable Elements

Field	Description
MailstorePath	Outlook files in AppData\Local\Comms\Unistore\data
TransportRuleNames	Target suspicious rule changes (e.g., header removal)
PowerShellCommandMatch	Regex match on `Remove-MailboxExportRequest` and similar Exchange cmdlets

AN0738

Detects the use of mail utilities like `mail` or `mailx` to delete mailbox content, or file-level deletion of inbox files from `/var/spool/mail/` or `/var/mail/` following suspicious sessions.

Log Sources

Mutable Elements

Field	Description
MailFolderPath	Common inbox file locations like /var/spool/mail/, /var/mail/
CommandPattern	Usage of mailx or echo piped to mail followed by deletion

AN0739

Detects removal of Apple Mail artifacts via AppleScript or direct deletion of mailbox content in ~/Library/Mail/, especially when preceded by Remote Login or C2-related API access.

Log Sources

Mutable Elements

Field	Description
ScriptCommandMatch	AppleScript references to Mail.app and delete commands
LibraryPathMatch	Files within ~/Library/Mail/V*/ folders

AN0740

Detects Exchange Online or on-prem transport rule changes (e.g., header stripping) and mailbox export cleanup via `Remove-MailboxExportRequest`, as well as admin actions via Exchange PowerShell sessions.

Log Sources

Mutable Elements

Field	Description
CmdletFilter	Include `New-TransportRule`, `Set-TransportRule`, `Remove-*` actions
UserRoleScope	Track role assignments for admins performing deletions

---