Indicator Removal: Clear Mailbox Data, Sub-technique T1070.008 - Enterprise

Archived: 2026-04-05 17:45:03 UTC

Adversaries may modify mail and mail application data to remove evidence of their activity. Email applications allow users and other programs to export and delete mailbox data via command line tools or use of APIs. Mail application data can be emails, email metadata, or logs generated by the application or operating system, such as export requests.

Adversaries may manipulate emails and mailbox data to remove logs, artifacts, and metadata, such as evidence of Phishing/Internal Spearphishing, Email Collection, Mail Protocols for command and control, or email-based exfiltration such as Exfiltration Over Alternative Protocol. For example, to remove evidence on Exchange servers adversaries have used the `ExchangePowerShell` PowerShell module, including `Remove-MailboxExportRequest` to remove evidence of mailbox exports.[1][2] On Linux and macOS, adversaries may also delete emails through a command line utility called `mail` or use AppleScript to interact with APIs on macOS.[3][4]

Adversaries may also remove emails and metadata/headers indicative of spam or suspicious activity (for example, through the use of organization-wide transport rules) to reduce the likelihood of malicious emails being detected by security products.[5]

Source: https://attack.mitre.org/techniques/T1070/008