Hide Artifacts: Email Hiding Rules, Sub-technique T1564.008 - Enterprise

Archived: 2026-04-05 18:25:49 UTC

Adversaries may use email rules to hide inbound emails in a compromised user's mailbox. Many email clients allow users to create inbox rules for various email functions, including moving emails to other folders, marking emails as read, or deleting emails. Rules may be created or modified within email clients or through external features such as the `New-InboxRule` or `Set-InboxRule` PowerShell cmdlets on Windows systems.[1][2][3][4]

Adversaries may utilize email rules within a compromised user's mailbox to delete and/or move emails to less noticeable folders. Adversaries may do this to hide security alerts, C2 communication, or responses to Internal Spearphishing emails sent from the compromised account.

Any user or administrator within the organization (or adversary with valid credentials) may be able to create rules to automatically move or delete emails. These rules can be abused to impair/delay detection had the email content been immediately seen by a user or defender. Malicious rules commonly filter out emails based on key words (such as `malware`, `suspicious`, `phish`, and `hack`) found in message bodies and subject lines. [5]

In some environments, administrators may be able to enable email rules that operate organization-wide rather than on individual inboxes. For example, Microsoft Exchange supports transport rules that evaluate all mail an organization receives against user-specified conditions, then performs a user-specified action on mail that adheres to those conditions.[6] Adversaries that abuse such features may be able to automatically modify or delete all emails related to specific topics (such as internal security incident notifications).

Source: https://attack.mitre.org/techniques/T1564/008