Hunting for email forwarding rules compromise in Exchange

Author: mdecrevoisier
Version: 2022.08.28
Status: stable

Sources:
- Redcanary: https://redcanary.com/blog/email-forwarding-rules/
- Exchange PowerShell: https://docs.microsoft.com/en-us/powershell/module/exchange/?view=exchange-ps
- Exchange EWS rules: https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-manage-inbox-rules-by-using-ews-in-exchange
- Azure Graph API rules: https://docs.microsoft.com/en-us/graph/api/mailfolder-post-messagerules?view=graph-rest-1.0&tabs=http

Rule manipulation sources

Source

- Exchange Server
  - Exchange Web Services (EWS) — API
  - Exchange Management Shell (EMS) — PowerShell
  - Exchange Admin Center (EAC) — Web access
  - Outlook Web Access (OWA) — Web access
- Exchange online
  - Exchange Web Services (EWS) — API
  - Azure Graph — API
  - Exchange Online PowerShell — PowerShell
  - Exchange Admin Center (EAC) — Web access
  - Outlook Online — Web access
- Desktop client
  - Reported as "Client=MSExchangeRPC" — Outlook client

Operation

Triggered via Outlook online or PowerShell cmdlet

- New-InboxRule — Creation
- Set-InboxRule — Update
- Remove-InboxRule — Delete
- Enable-InboxRule — Status
- Disable-InboxRule — Status

Triggered via Outlook client using EWS API

- AddMailboxRule — UpdateInboxRules — Creation & Update
- ModifyMailboxRule — UpdateInboxRules — Creation & Update

Triggered via PowerShell or OWA

- Set-Mailbox — Update

Rule settings definition

Condition

- Email sender
  - From
  - FromAddressContainsWords
- Recipient
  - SentTo
  - SentOnlyToMe
  - RecipientAddressContainsWords
- Subject
  - SubjectContainsWords
  - SubjectOrBodyContainsWords
- Body
  - BodyContainsWords
  - SubjectOrBodyContainsWords
- Importance
  - WithImportance
- Size
  - WithinSizeRangeMinimum
  - WithinSizeRangeMaximum
- Attachment
  - HasAttachment

Action

- Forward
  - ForwardTo
  - ForwardAsAttachmentTo
  - ForwardingSmtpAddress — Triggered only via command "Set-Mailbox"
  - ForwardingAddress — Triggered only via command "Set-Mailbox"
- Redirect
  - RedirectTo
- Copy
  - CopyToFolder
- Move
  - MoveToFolder
- Delete
  - SoftDeleteMessage
  - DeleteMessage
- Mark as read
  - MarkAsRead

Destination

- Internal
  - Folder
    - Deleted ilems — May be suspicious
    - Rss Feeds — May be suspicious
    - RSS Subscriptions — May be suspicious
    - Archive — May be suspicious
    - Custom — May be suspicious
  - Recipient
- External
  - External domain recipient — May be suspicious

Rules logs locations

Placeholder

- Exchange online
  - Office 365 Management Activity API
  - Security Graph API — Defender for Cloud App (ex-MCAS)
- Exchange Server
  - Mailbox audit logs — Requires advanced auditing activation