Hunting for email forwarding rules compromise in Exchange

Author: mdecrevoisier
Version: 2022.08.25
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
  - API
    - Exchange Web Services (EWS)
    - Azure Graph
  - Desktop client
    - Outlook client
  - PowerShell
    - Exchange Management Shell (EMS)
    - Exchange Online PowerShell
  - Web access
    - Exchange Admin Center (EAC)
    - Outlook Web Access (OWA)
    - Outlook online
- Commands
  - EWS
    - New-InboxRule — Creation
    - UpdateInboxRules — Creation & Update
    - Set-InboxRule
  - Set-Mailbox — Update
  - Remove-InboxRule — Delete
  - Enable-InboxRule — Status
  - Disable-InboxRule

Forwarding 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
    - -ForwardingAddress

    Triggered only with command "Set-Mailbox"
  - Redirect
    - -RedirectTo
  - Copy
    - -CopyToFolder
  - Move
    - -MoveToFolder
  - Delete
    - -SoftDeleteMessage
    - -DeleteMessage
  - Mark as read
    - -MarkAsRead
- Destination
  - Internal
    - Folder
      - Deleted items
      - RSS Feeds
      - Archived
      - Custom

      May be suspicious
    - Recipient
  - External
    - External domain recipient

      May be suspicious