Hunting for email forwarding rules compromise in Exchange

Rules manipulation sources

- Source
  - Exchange Server
    - API: Exchange Web Services (EWS)
    - PowerShell: Exchange Management Shell (EMS)
    - Web access: Exchange Admin Center (EAC)
    - Web access: Outlook Web Access (OWA)
  - Exchange online
    - API: Exchange Web Services (EWS)
    - API: Azure Graph
    - PowerShell: Exchange Online PowerShell
    - Web access: Exchange Admin Center (EAC)
    - Web access: Outlook online
  - Desktop client
    - Outlook client: Reported as "Client=MSExchangeRPC"
- Operation
  - Triggered via Outlook online or PowerShell
    - Creation: New-InboxRule
    - Update: Set-InboxRule
    - Delete: Remove-InboxRule
    - Status: Enable-InboxRule
    - Status: Disable-InboxRule
  - Triggered via Outlook client using EWS API
    - UpdateInboxRules: AddMailboxRule
    - UpdateInboxRules: ModifyMailboxRule
    - Creation & Update: UpdateInboxRules
  - Triggered via OWA or PowerShell
    - Update: Set-Mailbox
    - Can only be used to forward all emails to another address (no move, copy or delete...)

Rules settings definition

- Condition
  - Email sender: From
  - Email sender: FromAddressContainsWords
  - Recipient: SentTo
  - Recipient: SentOnlyToMe
  - Recipient: RecipientAddressContainsWords
  - Subject: SubjectContainsWords
  - Subject: SubjectOrBodyContainsWords
  - Body: BodyContainsWords
  - Body: SubjectOrBodyContainsWords
  - Importance: WithImportance
  - Size: WithinSizeRangeMinimum
  - Size: WithinSizeRangeMaximum
  - Attachment: HasAttachment
- Action
  - Transfer
    - RedirectTo
    - ForwardTo
    - ForwardAsAttachmentTo
    - ForwardingSmtpAddress
    - ForwardingAddress (internal)
    - DeliverToMailboxAndForward
    - Arguments available only for command "Set-Mailbox"
  - Copy: CopyToFolder
  - Move: MoveToFolder
  - Delete
    - SoftDeleteMessage
    - DeleteMessage
  - Mark as read: MarkAsRead
- Destination
  - Internal
    - Folder
      - Deleted ilems
      - Rss Feeds
      - RSS Subscriptions
      - Archive
      - 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)
      - Reports suspicious rules creation
  - Exchange Server
    - Mailbox audit logs
    - Requires advanced auditing activation

Rule detection scenarios

- Scenarios
  - 1-Forwarding to external domain
    - ForwardTo
    - ForwardAsAttachmentTo
    - RedirectTo
    - Excluded
      - SubjectOrBodyContainsWords
      - SubjectContainsWords
      - BodyContainsWords
  - 2-Sniffing forwarding
    - SubjectOrBodyContainsWords
    - SubjectContainsWords
    - BodyContainsWords
    - Includes
      - ForwardTo
      - ForwardAsAttachmentTo
      - RedirectTo
  - 3-Hidding emails via deletion
    - SoftDeleteMessage
    - DeleteMessage
  - 4-Hidding emails via move or copy
    - MoveToFolder / CopyToFolder
      - Deleted items
      - Rss Feeds
      - RSS Subscriptions
      - Archive
  - 5-Email attachment (focus)
    - HasAttachment
    - WithinSizeRangeMinimum
    - WithinSizeRangeMaximum
  - 6-On behalf of user (focus)
  - 7-Short name (focus)
  - 8-Forwarding rule company breach
  - Hidden rule creation

Author: mdecrevoisier
Version: 2022.08.30
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