Hunting for email forwarding rules compromise in Exchange

Exchange

Rules manipulation sources

Vectors

- Exchange Server
  - API
    - Exchange Web Services (EWS)
  - PowerShell
    - Exchange Management Shell (EMS)
  - Web access
    - Exchange Admin Center (EAC)
    - Outlook on the web (formerly known as Outlook Web App or Outlook Web Access / OWA)
- Exchange online
  - API
    - Exchange Web Services (EWS)
    - Azure Graph
  - PowerShell
    - Exchange Online PowerShell
  - Web access
    - Exchange Admin Center (EAC)
    - Outlook on the web (formerly known as Outlook Web App or Outlook Web Access / OWA)
- Desktop client
  - Outlook client
    - Reported as "Client=MSExchangeRPC"

Operations

Triggered via Outlook online or PowerShell

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

Triggered via Outlook client using EWS API

- Creation & Update
  - UpdateInboxRules
    - AddMailboxRule
    - ModifyMailboxRule

Triggered via OWA or PowerShell

- Update
  - Set-Mailbox
    - Can only be used to forward all emails to another address (no move, copy nor delete...)

Rules settings definition

Conditions

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

Actions

- 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
    - Conversation history
    - 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

Author: mdecrevoisier
Version: 2022.09.04
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
- https://raw.githubusercontent.com/PwC-IR/Business-Email-Compromise-Guide/main/PwC-Business_Email_Compromise-Guide.pdf
- https://docs.microsoft.com/en-us/microsoft-365/security/defender/alert-grading-playbook-email-forwarding?view=o365-worldwide
- https://logrhythm.com/blog/detecting-and-preventing-auto-forwarding-and-phishing-attacks-in-office-365/