Hunting for email forwarding rules compromise in Exchange

Author: mdecrevoisier
Version: 2022.09.07
Status: stable

Sources:
- Redcanary: https://redcanary.com/blog/email-forwarding-rules/
- https://raw.githubusercontent.com/PwC-IR/Business-Email-Compromise-Guide/main/PwC-Business_Email_Compromise-Guide.pdf
- https://logrhythm.com/blog/detecting-and-preventing-auto-forwarding-and-phishing-attacks-in-office-365/
- https://www.sans.org/blog/sans-data-incident-2020-indicators-of-compromise/

- 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://docs.microsoft.com/en-us/microsoft-365/security/defender/alert-grading-playbook-email-forwarding?view=o365-worldwide

Rules manipulation sources

Vectors

- Exchange Server
  - Exchange Web Services (EWS) — API
  - Exchange Management Shell (EMS) — PowerShell
  - Exchange Admin Center (EAC) — Web access
  - Outlook on the web (formerly known as Outlook Web App or Outlook Web Access / OWA) — Web access
- Exchange online
  - Exchange Web Services (EWS) — API
  - Azure Graph — API
  - Office 365 app — API (See SANS link source)
  - Exchange Online PowerShell — PowerShell
  - Exchange Admin Center (EAC) — Web access
  - Outlook on the web (formerly known as Outlook Web App or Outlook Web Access / OWA) — Web access
- Desktop client
  - Outlook client — Reported as "Client=MSExchangeRPC"

Operations

Triggered via Outlook online, PowerShell or Graph API

- 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 OWA or PowerShell

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

Rule detection scenarios

Scenarios

- 1-Forwarding to external domain
  - ForwardTo
  - ForwardAsAttachmentTo
  - RedirectTo
  - Excludes
    - SubjectOrBodyContainsWords
    - SubjectContainsWords
    - BodyContainsWords
- 2-Sniffing forwarding to external domain
  - ForwardTo
  - ForwardAsAttachmentTo
  - RedirectTo
  - Includes
    - SubjectOrBodyContainsWords
    - SubjectContainsWords
    - BodyContainsWords
- 3-Hidding emails via deletion
  - SoftDeleteMessage
  - DeleteMessage
- 4-Hidding emails via move
  - MoveToFolder
    - Deleted items
    - Rss Feeds
    - RSS Subscriptions
    - Conversation history
    - Archive
    - Junk emails
- 5-Email attachment (focus)
  - HasAttachment
  - WithinSizeRangeMinimum
  - WithinSizeRangeMaximum
- 6-On behalf of user (focus)
- 7-Short name (focus)
- 8-Forwarding rule company breach
- 9-Suspicious login followed by rule creation
- 10-Hidden rule creation

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
- Mark as read — MarkAsRead
- RuleCondition
  - Actions from command "UpdateInboxRules" are triggered on Outlook for desktop and are reported in a different structure

Destination

- Internal
  - Folder
    - Deleted ilems
    - Rss Feeds
    - RSS Subscriptions
    - Conversation history
    - Archive
    - Junk emails
    - 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