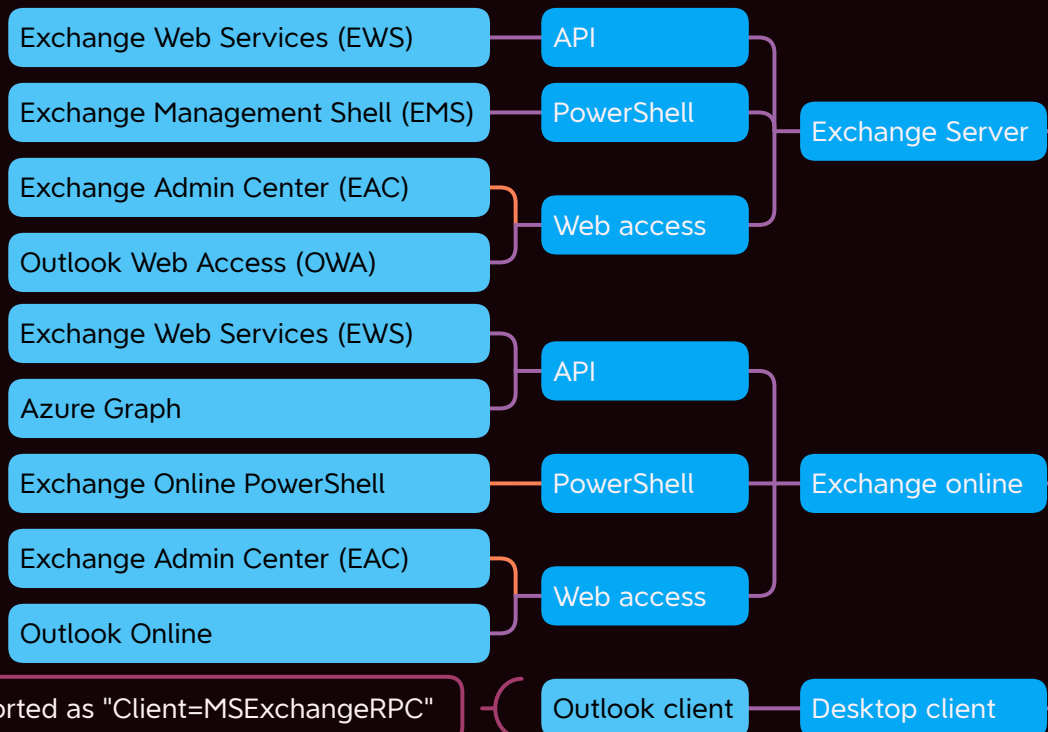


Hunting for email forwarding rules compromise in Exchange

Source

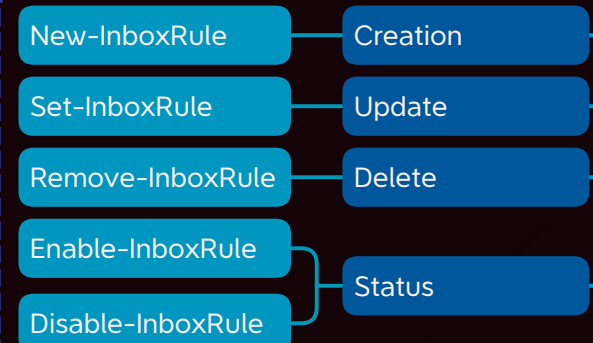
Rule manipulation sources



Reported as "Client=MSExchangeRPC"

Operation

Triggered via Outlook online or PowerShell cmdlet



Triggered via Outlook client using EWS API



Triggered via PowerShell or OWA

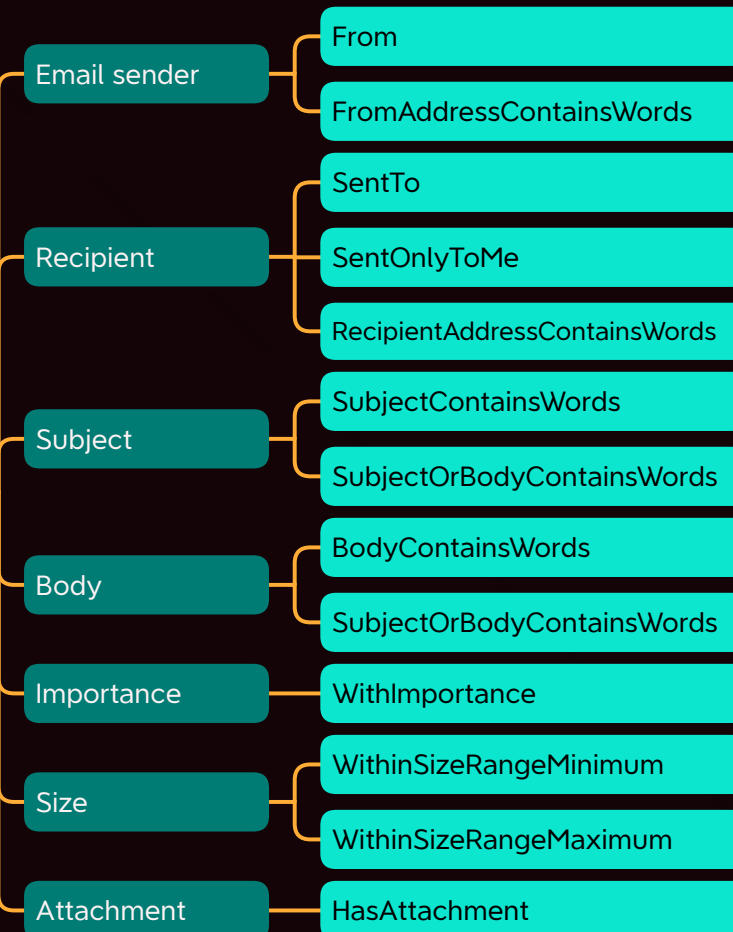


Author: mdecrevoisier
Version: 2022.08.28
Status: stable

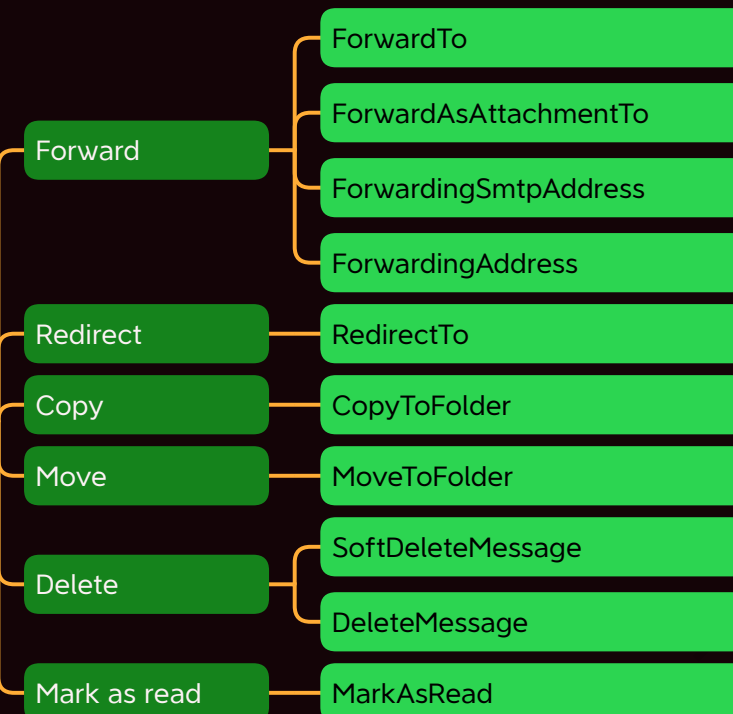
Sources:
- Redcanary: <https://redcanary.com/blog/email-forwarding-rules/>
- Exchange PowerShell: <https://docs.microsoft.com/en-us/powershell/module/exchange/?view=exchange-ps>
- Exchange EWS rules: <https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-manage-inbox-rules-by-using-ews-in-exchange>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

Rule settings definition

Condition

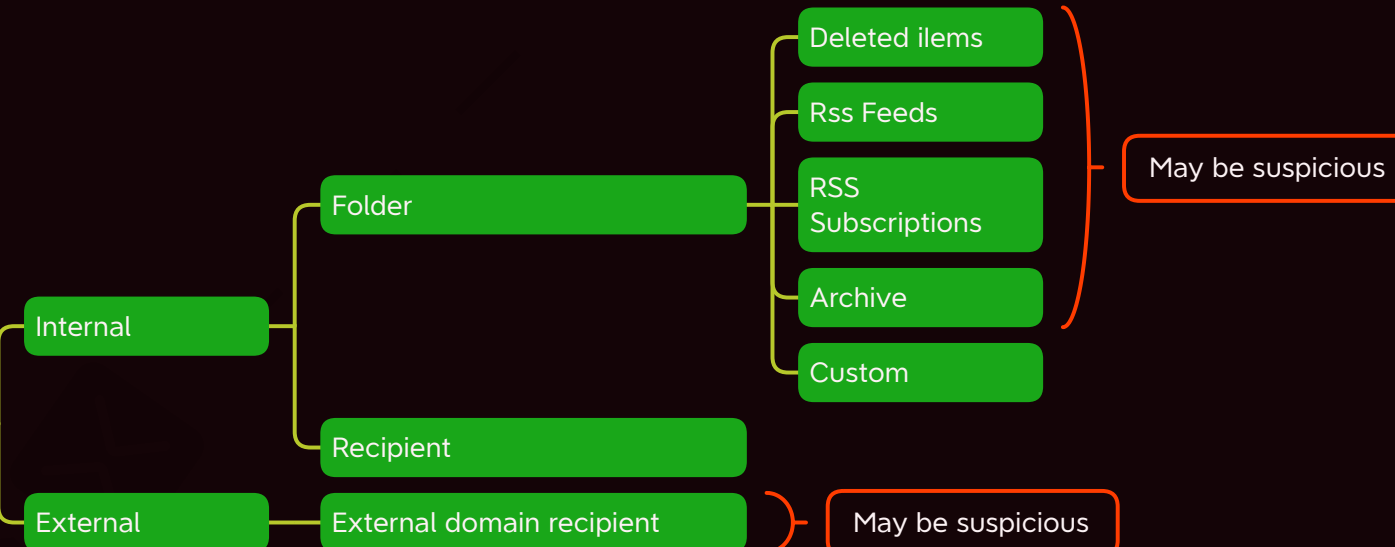


Action



Triggered only via command "Set-Mailbox"

Destination



May be suspicious

May be suspicious

Rules logs locations

Placeholder

