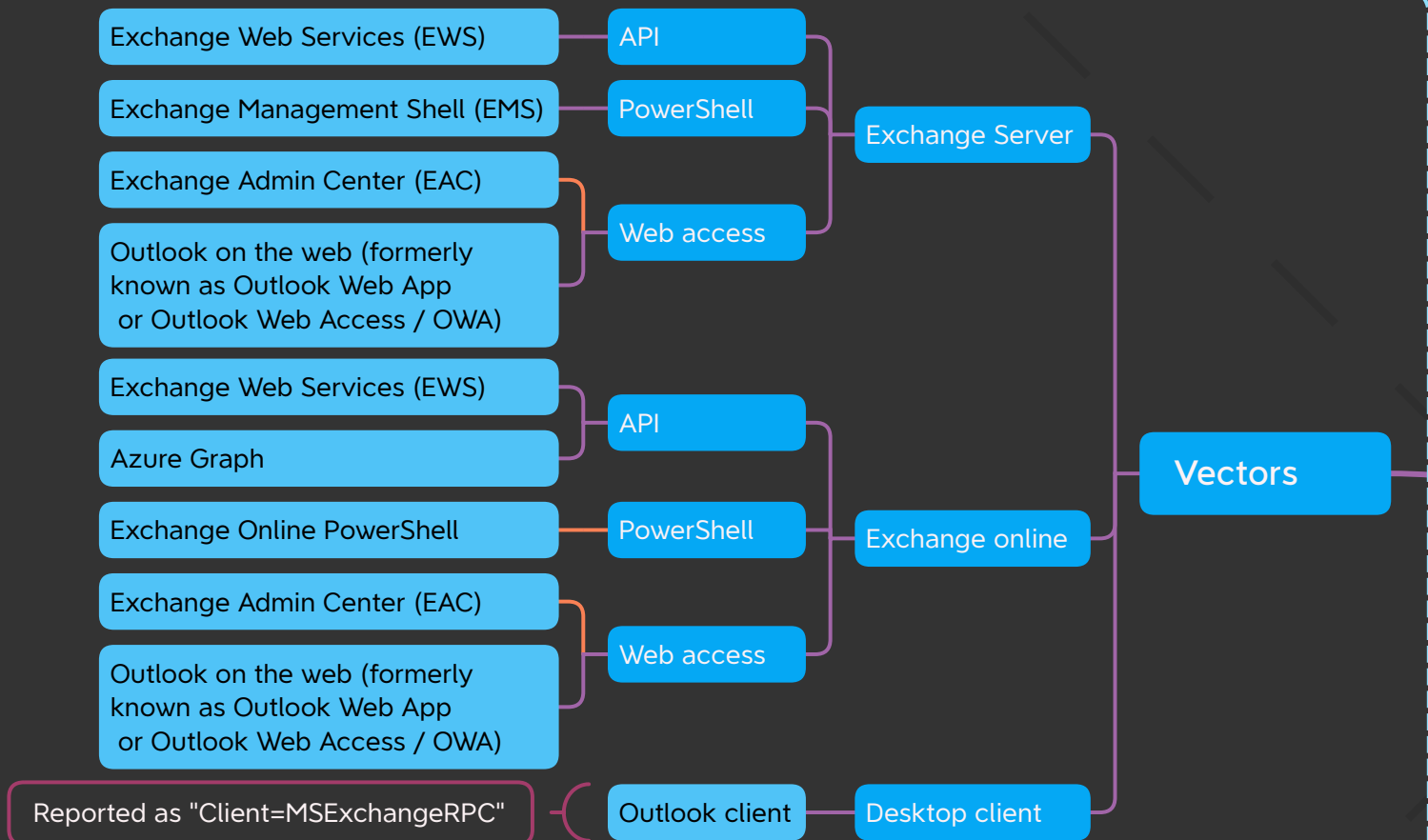




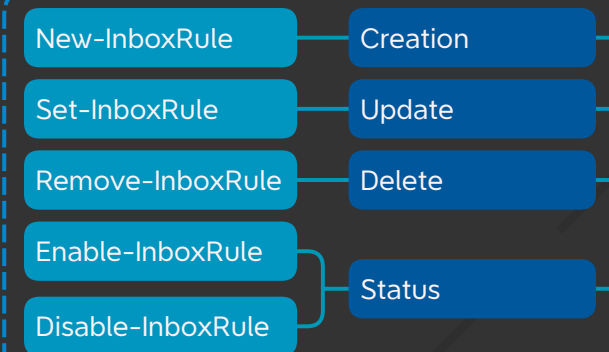
Hunting for email forwarding rules compromise in Exchange

Rules manipulation sources



Vectors

Triggered via Outlook online or PowerShell



Triggered via Outlook client using EWS API

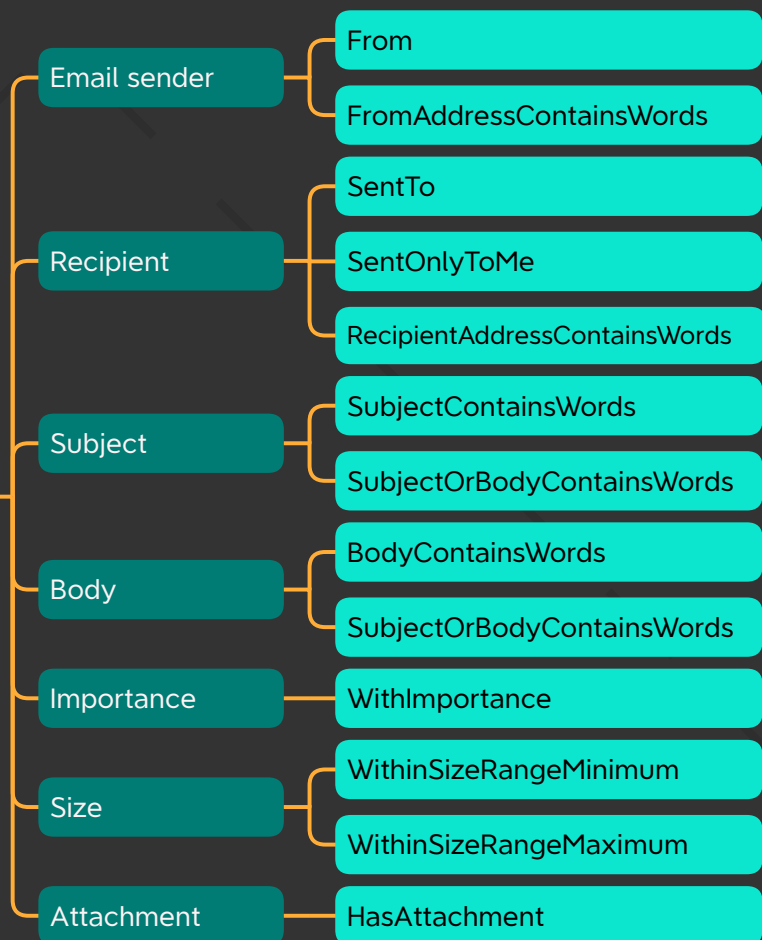


Triggered via OWA or PowerShell

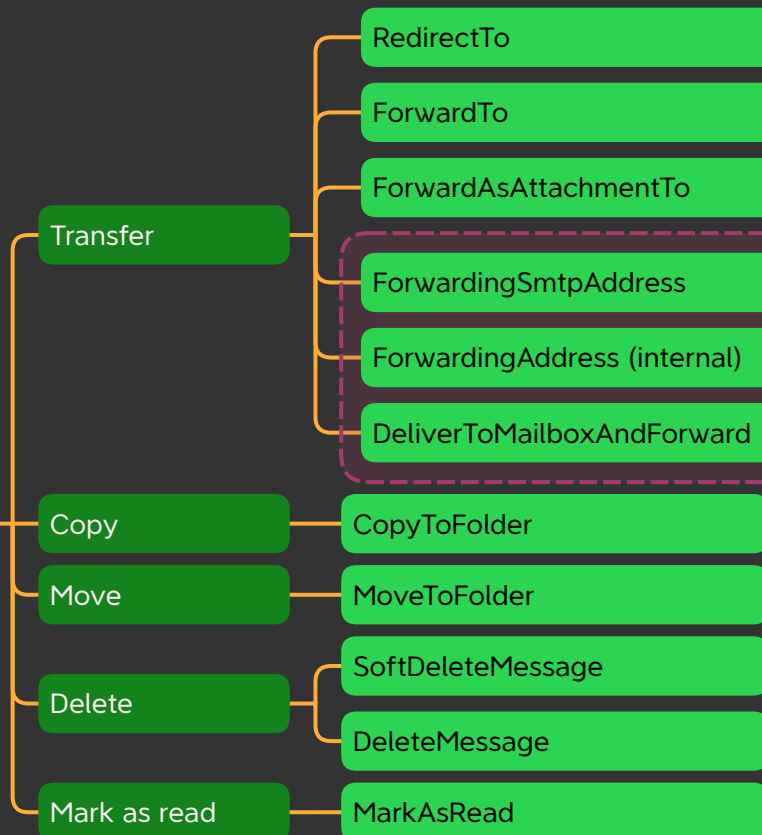


Operations

Conditions

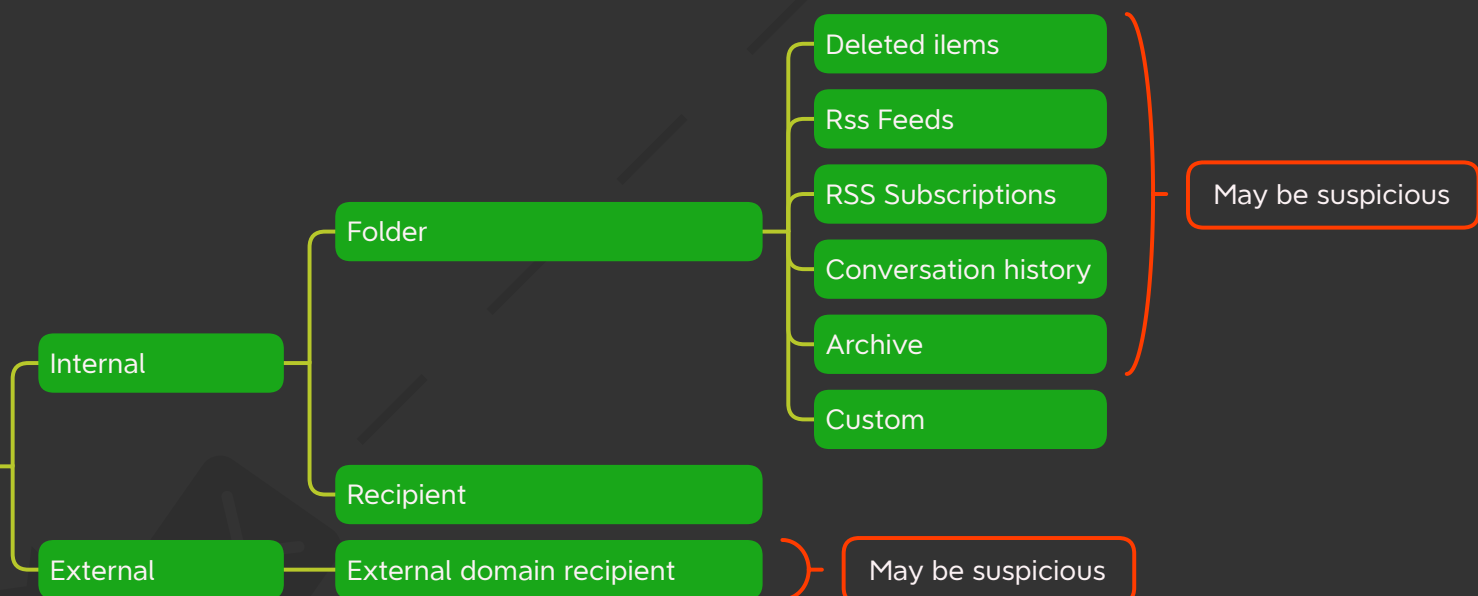


Actions



Arguments available only for command "Set-Mailbox"

Destination



Rules logs locations

Placeholder



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-messengerules?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/>