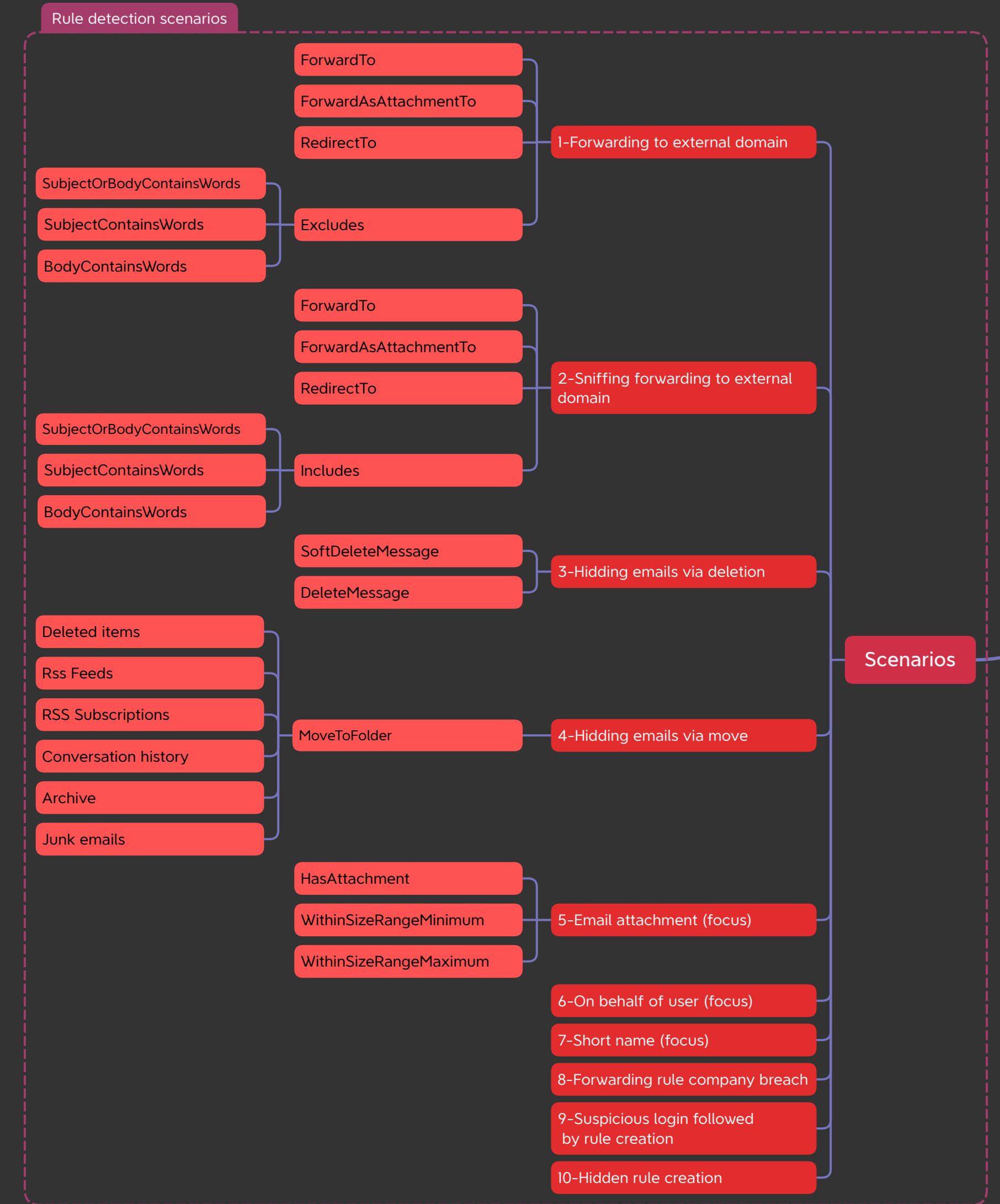
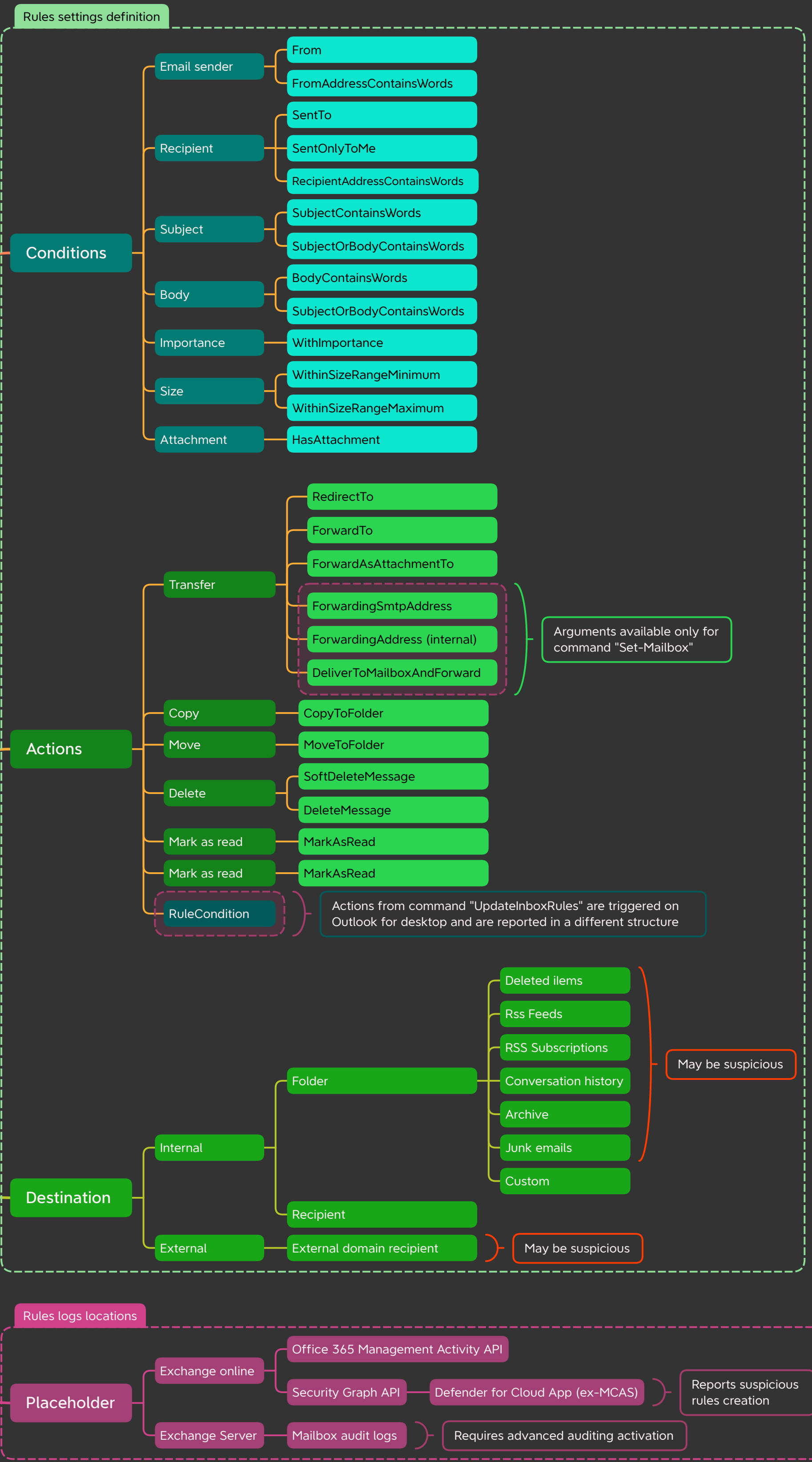


Hunting for email rules compromise in Exchange and Office 365



Author: mdecrevoisier
Version: 2022.11.10
Status: stable

Sources:

- Redcanary: <https://redcanary.com/blog/o365-email-rules-mindmap/>
- 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>