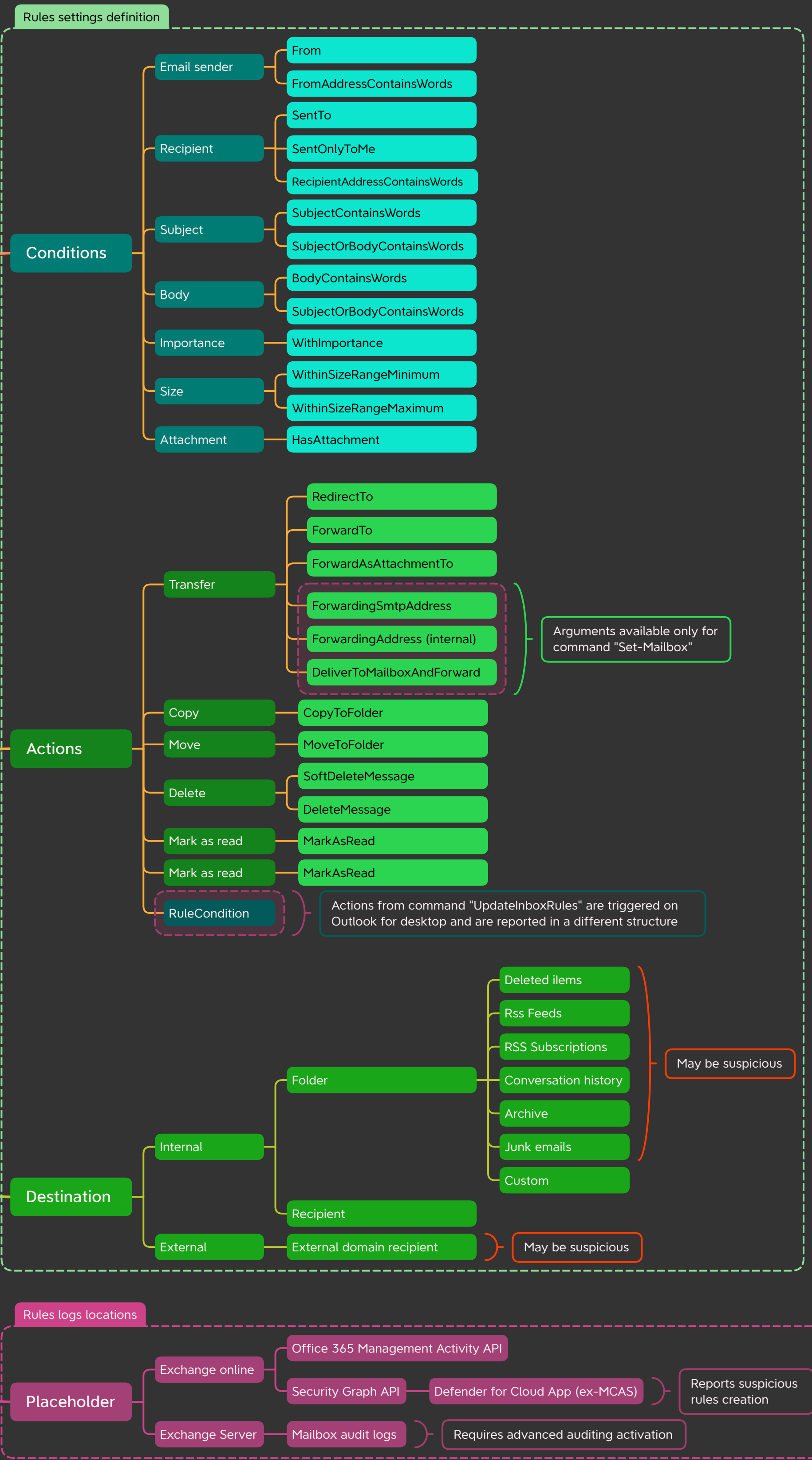


## Hunting for email forwarding rules compromise in Exchange



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://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>