

Office Application Startup: Outlook Rules, Sub-technique T1137.005 - Enterprise

Archived: 2026-04-05 14:26:31 UTC

Adversaries may abuse Microsoft Outlook rules to obtain persistence on a compromised system. Outlook rules allow a user to define automated behavior to manage email messages. A benign rule might, for example, automatically move an email to a particular folder in Outlook if it contains specific words from a specific sender. Malicious Outlook rules can be created that can trigger code execution when an adversary sends a specifically crafted email to that user. [\[1\]](#)

Once malicious rules have been added to the user's mailbox, they will be loaded when Outlook is started. Malicious rules will execute when an adversary sends a specifically crafted email to the user. [\[1\]](#)

Source: <https://attack.mitre.org/techniques/T1137/005>