Detect Persistence via Malicious Outlook Rules, Detection Strategy DET0095

Archived: 2026-04-05 13:46:47 UTC

AN0263

Adversary uses a tool like Ruler or MFCMapi to create a malicious Outlook rule that triggers execution upon receipt of a crafted email. On email delivery, Outlook executes the rule, resulting in code execution (e.g., launching mshta.exe or PowerShell). Outlook spawns a non-standard child process, often unsanctioned, without user interaction.

Log Sources

Mutable Elements

Field	Description
ChildProcessName	Outlook may spawn mshta.exe, powershell.exe, or wscript.exe depending on attacker payload
RuleTriggerCondition	Rule execution may depend on message subject, sender, or message header content
ParentProcessName	Legitimate Outlook activity should not spawn scripting or interpreter processes
TimeWindow	Execution may occur with delay after message receipt or folder interaction

AN0264

Adversary adds a new Outlook rule with modified or obfuscated PR_RULE_MSG_NAME and PR_RULE_MSG_PROVIDER attributes using MFCMapi or Ruler. Rule is triggered when email arrives, executing embedded or external code. Mailbox audit logs or Unified Audit Log shows automated rule-triggered action without user interaction.

Log Sources

Mutable Elements

Field	Description
AuditPolicyScope	Mailbox rule changes may not be captured unless advanced audit logging is enabled

Field	Description
RuleProviderName	Malicious rules may use spoofed or non-standard PR_RULE_MSG_PROVIDER values
TriggerSubjectKeywords	Triggering emails may contain uncommon but benign-looking subjects
UserContext	Target user account may be inactive or high-value (e.g., VIP, service account)

Source: https://attack.mitre.org/detectionstrategies/DET0095