Detection Strategy for Email Hiding Rules, Detection Strategy DET0192

Archived: 2026-04-05 16:40:21 UTC

AN0551

Suspicious creation or modification of inbox rules through PowerShell (New-InboxRule, Set-InboxRule) to automatically delete, move, or hide emails. Defender perspective: unusual rule activity correlated with mailbox access and filtering patterns.

Log Sources

Mutable Elements

Field	Description
SuspiciousKeywords	Keywords like 'phish', 'malware', 'suspicious' used in inbox rules to hide emails.
UserContext	Scope mailbox monitoring to high-value users such as executives or admins.

AN0552

Alterations to plist configuration files (RulesActiveState.plist, SyncedRules.plist, UnsyncedRules.plist, MessageRules.plist) that define email hiding or filtering rules. Defender perspective: unexpected changes in these files associated with Mail.app processes.

Log Sources

Mutable Elements

Field	Description
WatchedPlistFiles	Adjust to monitor only rule-related plist files relevant to the environment.

AN0553

Rule manipulation through local email clients (e.g., Evolution, Thunderbird) or server-side filtering scripts (e.g., sieve) creating conditions to move or discard emails with security-related keywords.

Log Sources

Mutable Elements

Field	Description
MailServerLogs	Customize based on mail server software (Postfix, Dovecot, Exim).

AN0554

Suspicious rule creation within Outlook or Exchange clients, including auto-move or delete conditions tied to incident or security alert keywords. Defender perspective: correlation between missing inbound emails and newly added mailbox rules.

Log Sources

Mutable Elements

Field	Description
RuleScope	Decide whether to monitor individual mailbox rules, org-wide transport rules, or both.
