Email Collection via Local Email Access and Auto-Forwarding Behavior, Detection Strategy DET0476

Archived: 2026-04-02 12:22:18 UTC

AN1309

Correlates creation of email forwarding rules or header anomalies (e.g., X-MS-Exchange-Organization-AutoForwarded) with suspicious process execution, file access of .pst/.ost files, and network connections to external SMTP servers.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines correlation window across email rule creation and outbound SMTP.
UserContext	Filters for admin or service accounts to reduce false positives.
SMTPDomainList	Allows tuning based on expected external email domains.

AN1310

Detects file access to mbox/maildir files in conjunction with curl/wget/postfix execution, or anomalous shell scripts harvesting user mail directories.

Log Sources

Mutable Elements

Field	Description
WatchedMailDirs	Specify user mail directories (/var/mail, ~/Maildir)
ProcessNameList	Tune based on local mail clients or curl usage in environment
TimeWindow	Define how close together access and exfil events must occur

AN1311

Monitors Mail.app database or maildir file access, automation via AppleScript, and abnormal mail rule creation using scripting or UI automation frameworks.

Log Sources

Mutable Elements

Field	Description
ScriptProcessNameList	Script interpreters or automation tools (osascript, Automator, etc.)
WatchedMailFiles	Mail.app SQLite DB or .emlx directory

AN1312

Correlates unusual auto-forwarding rule creation via Exchange Web Services or Outlook rules engine, presence of X-MS-Exchange-Organization-AutoForwarded headers, and logon session anomalies from abnormal IPs.

Log Sources

Mutable Elements

Field	Description
UserAgentList	Restrict rules from non-browser agents
ExternalSMTPDomainList	Allow listing for org-sanctioned forwarding domains
TimeWindow	Time delta between rule creation and suspicious sign-in

---