Detection of Mail Protocol-Based C2 Activity (SMTP, IMAP, POP3), Detection Strategy DET0135

Archived: 2026-04-05 13:37:21 UTC

AN0379

Detects unauthorized use of SMTP/IMAP/POP3 by suspicious binaries (e.g., PowerShell, rundll32) to exfiltrate data or beacon via email, often bypassing proxy or content filters.

Log Sources

Mutable Elements

Field	Description
ProcessImageName	Limit to uncommon clients (e.g., scripts or CLI tools using .NET SMTP libraries)
DestPortFilter	Typically 25, 587, 993, 995, or 465 – flag anomalies
AttachmentType	Flag suspicious attachments (e.g., .zip, .7z, .bin)

AN0380

Detects non-interactive or script-driven email transmission using tools like `sendmail`, `mailx`, or custom SMTP scripts by background processes, especially when sending attachments or large payloads.

Log Sources

Mutable Elements

Field	Description
TransferSizeThreshold	Bytes transferred via SMTP session
ScriptNameFilter	e.g., base64 encoded mailer scripts or one-liners in cron

AN0381

Detects email-sending behavior via Terminal, AppleScript, or Automator that interfaces with SMTP or IMAP, typically using curl or mail-related APIs in unsanctioned contexts.

Log Sources

Mutable Elements

Field	Description
UserContext	Monitor non-mail client users initiating SMTP/IMAP
TimeWindow	Look for execution of mail commands during off-hours

AN0382

Detects hosts transmitting large volumes of SMTP, IMAP, or POP3 traffic to external IPs or relays that aren't associated with the enterprise mail infrastructure.

Log Sources

Mutable Elements

Field	Description
ExternalMailRelayFilter	Dest IPs not matching sanctioned SMTP/IMAP relays
OutflowToInflowRatio	Outbound email bytes vastly exceed response

---