Detect Remote Email Collection via Abnormal Login and Programmatic Access, Detection Strategy DET0048

Archived: 2026-04-02 11:15:46 UTC

AN0131

Detects adversaries accessing remote mail systems (e.g., Exchange Online, O365) using stolen credentials or OAuth tokens, followed by scripted access to mailbox contents via PowerShell, AADInternals, or unattended API queries. Detection focuses on abnormal logon sessions, user agents, IP locations, and scripted or tool-based email data access.

Log Sources

Mutable Elements

Field	Description
UserAgentPattern	Filters user agents like 'PowerShell', 'AADInternals', 'python-requests' which can vary depending on script/tool.
TimeWindow	Defines the temporal correlation window between login, command execution, and outbound email access.
KnownIPLocations	Defines baseline geo/IP address ranges to suppress known corporate access.
PrivilegedUserList	Defines the accounts considered privileged (admin, execs) and worthy of tighter thresholds.

AN0132

Monitors programmatic access to user mailboxes in cloud-based email systems (e.g., O365, Exchange Online) using APIs or tokens. Focuses on OAuth misuse, suspicious MailItemsAccessed patterns, scripted keyword searches, and connections from untrusted agents or locations.

Log Sources

Mutable Elements

Field	Description
MailAccessVolumeThreshold	Number of emails accessed within time window to flag anomaly.

Field	Description
OAuthClientIDAllowList	Allows tuning based on known app registrations.
KeywordSearchFrequency	Flag high volumes of message searches using suspicious patterns.
LoginGeolocationVariance	Trigger when IP geolocation varies significantly from user's historical profile.

Source: https://attack.mitre.org/detectionstrategies/DET0048#AN0132