Detect Local Email Collection via Outlook Data File Access and Command Line Tooling, Detection Strategy DET0047

Archived: 2026-04-05 12:55:37 UTC

AN0130

Detection focuses on processes that attempt to locate, access, or exfiltrate local Outlook data files (.pst/.ost) using file system access, native Windows utilities (e.g., PowerShell, WMI), or remote access tools with file browsing capabilities. The behavior chain includes directory enumeration, file access, optional compression or staging, and network transfer.

Log Sources

Mutable Elements

Field	Description
TargetFilePathPattern	Regex or wildcard patterns for sensitive Outlook file paths (.ost/.pst) depending on organizational deployment.
TimeWindow	Timeframe used to correlate related file access, process creation, and exfiltration events.
UserContext	Limit detection to user accounts not normally interacting with Outlook file locations (e.g., service accounts, low-privileged users).
ProcessAllowList	Filter known legitimate Outlook-accessing processes to reduce false positives.
