Detect Suspicious Access to Windows Credential Manager, Detection Strategy DET0134

Archived: 2026-04-05 17:27:28 UTC

AN0378

Detects unauthorized access to Windows Credential Manager through anomalous process execution (vaultcmd.exe, rundll32.exe keymgr.dll), suspicious API calls (CredEnumerateA), or direct file access to Credential Locker files. Correlates process creation with subsequent file reads of .vcrd/.vpol files under user Credential Locker directories.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	Credential Locker paths such as %Systemdrive%\Users*\AppData\Local\Microsoft\Credentials and %Systemdrive%\Users*\AppData\Local\Microsoft\Vault
TimeWindow	Correlation window between process execution, file access, and API calls
PrivilegedUsers	Baseline of expected administrative/service accounts with legitimate Credential Manager access