Detect Credential Discovery via Windows Registry Enumeration, Detection Strategy DET0250

Archived: 2026-04-05 17:42:02 UTC

AN0694

Defenders observe command-line executions or API-based registry reads targeting sensitive paths like HKLM or HKCU with keyword filters such as 'password', 'cred', or 'logon'. Typically performed by Reg.exe, PowerShell, custom binaries, or offensive tools such as Cobalt Strike. Correlation with process ancestry and command-line arguments indicates suspicious credential discovery activity.

Log Sources

Mutable Elements

Field	Description
KeywordMatch	List of strings searched in registry queries (e.g., password, credential, login). May need to expand for localized OS or app-specific terms.
ParentProcessFilter	Parent process used for registry access. Can tune for suspicious ancestry (e.g., cmd.exe > reg.exe vs. services.exe > reg.exe).
TimeWindow	Time-based correlation window for detecting chained activity between registry reads and subsequent credential use or exfiltration.
RegistryHiveScope	HKLM vs. HKCU vs. others. May limit scope to user or system context depending on risk appetite.
