Credential Dumping from SAM via Registry Dump and Local File Access, Detection Strategy DET0085

Archived: 2026-04-05 15:37:12 UTC

Analytics

- Windows

AN0235

An adversary running with SYSTEM-level privileges executes commands or accesses registry keys to dump the SAM hive or directly reads sensitive local files from the config directory. This behavior often involves sequential access to HKLM\SAM, HKLM\SYSTEM, and creation of .save or .dmp files, enabling offline hash extraction.

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	Detectable variations include `reg save`, `reg.exe save`, or PowerShell equivalents for dumping SAM/SYSTEM hives.
TargetFilePath	Defenders can tune based on dump file path patterns (e.g., `%TEMP%\sam.save`, `C:\Users\Public\*.dmp`).
RegistryPath	Tune for HKLM\SAM, HKLM\SYSTEM or access via direct \Device\Harddisk paths.
TimeWindow	Temporal gap between SAM and SYSTEM hive dumping can be tuned (e.g., 3 minutes).
ParentProcessName	Useful for suppressing known-good access (e.g., backup tools).