Detect Unauthorized Access to Password Managers, Detection Strategy DET0597

Archived: 2026-04-05 14:50:41 UTC

AN1641

Detection of suspicious access to password manager processes (KeePass, 1Password, LastPass, Bitwarden) through abnormal process injection, memory reads, or command-line usage of vault-related DLLs. Correlates process creation with OS API calls and file access to vault databases (.kdbx, .opvault, .ldb).

Log Sources

Mutable Elements

Field	Description
PasswordManagerBinaries	List of monitored binaries and file formats for password managers in use (e.g., KeePass, 1Password, Bitwarden, LastPass).
TimeWindow	Window to correlate process creation, API access, and file reads indicative of credential extraction.
UserContext	Filter for administrative accounts vs. expected users of password managers.

AN1642

Suspicious access to password manager vaults (KeePassXC, gnome-keyring, pass) via memory scraping or unauthorized file reads. Detects unusual command execution involving gdb/strace attached to password manager processes.

Log Sources

Mutable Elements

Field	Description
VaultFilePaths	Linux paths to monitor for vault database files (KeePassXC, pass, gnome-keyring).
TimeWindow	Correlation interval to detect multiple suspicious access events.

AN1643

Detection of password manager database access (1Password .opvault, LastPass caches, KeePass .kdbx) outside expected parent processes. Identifies memory scraping attempts via suspicious API calls or tools attaching to password manager processes.

Log Sources

Mutable Elements

Field	Description
VaultFileExtensions	Password manager file extensions (.opvault, .kdbx, .ldb) to monitor for anomalous access.
ParentProcessWhitelist	Expected parent processes that normally access password manager files, for filtering false positives.
