Detect Suspicious Access to Browser Credential Stores, Detection Strategy DET0037

Archived: 2026-04-05 16:23:07 UTC

AN0105

Detects unauthorized access to web browser credential stores (e.g., Chrome Login Data, Edge Credential Locker) by processes other than the browser itself. Correlates file reads of credential databases with subsequent API calls to `CryptUnprotectData` or memory inspection attempts.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	Browser-specific credential storage paths such as Chrome Login Data, IE Credential Locker
TimeWindow	Correlation window between file read and process memory/API access

AN0106

Detects attempts to access browser credential stores (e.g., Firefox `logins.json`, Chrome SQLite DB) or processes (e.g., gnome-keyring-daemon). Observes unauthorized file reads and memory inspection of browser processes using ptrace or gdb.

Log Sources

Mutable Elements

Field	Description
BrowserCredentialFiles	Paths of web browser credential databases to monitor
AllowedDebuggers	List of expected debugging tools for dev/test environments

AN0107

Detects abnormal access to Safari credential stores (Keychain-backed) or Chrome/Firefox login databases. Observes processes executing `security dump-keychain` or directly reading credential files in `~/Library/Application Support`. Correlates file access with suspicious process ancestry or unsigned binaries.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	execution of security, sqlite3, or unauthorized binaries
File Access (DC0055)	macos:unifiedlog	~/Library/Application Support/Google/Chrome/*/Login Data OR ~/Library/Application Support/Firefox/*/logins.json

Mutable Elements

Field	Description
PrivilegedUsers	Expected user context authorized to unlock Keychain or browser databases
TimeWindow	Correlation window for process execution and credential file access

---