Detection of Local Browser Artifact Access for Reconnaissance, Detection Strategy DET0013

Archived: 2026-04-05 17:26:45 UTC

AN0037

Access to browser artifact locations (e.g., Chrome, Edge, Firefox) by processes like PowerShell, cmd.exe, or unknown tools, followed by file reads, decoding, or export operations indicating enumeration of bookmarks, autofill, or history databases.

Log Sources

Mutable Elements

Field	Description
TargetPathRegex	Location of browser data folders like %APPDATA%\Google\Chrome\User Data or %APPDATA%\Mozilla\Firefox
ParentProcess	Used to exclude known browser maintenance or backup processes
ScriptBlockPattern	Used to detect suspicious PowerShell commands targeting browser data

AN0038

Unauthorized shell or script-based access to browser config or SQLite history files, typically in ~/.config/google-chrome/, ~/.mozilla/, or ~/.var/app folders, indicating enumeration of bookmarks or saved credentials.

Log Sources

Mutable Elements

Field	Description
BrowserProfilePath	User-specific browser data folders, e.g., ~/.config/chromium/Default/History
ShellRegex	Shell pattern detecting suspicious access to .sqlite or .json files

AN0039

Scripting or CLI tool access to ~/Library/Application Support/Google/Chrome or ~/Library/Safari bookmarks, cookies, or history databases. Detection relies on unexpected processes accessing or reading from these locations.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	macos:unifiedlog	Access to ~/Library/*/Safari or Chrome directories by non-browser processes
Process Creation (DC0032)	macos:osquery	process reading browser configuration paths

Mutable Elements

Field	Description
BrowserDBPath	System-specific paths to browser databases in user Library folders
NonBrowserProcessList	Processes not expected to touch browser DBs (e.g., curl, bash, python)
