Detect Access and Parsing of .bash_history Files for Credential Harvesting, Detection Strategy DET0385

Archived: 2026-04-05 16:16:24 UTC

AN1085

A process outside of interactive shell context reads ~/.bash_history directly (e.g., using cat, less, grep), often shortly after privilege escalation or user switch (su/sudo). This may be followed by credential scanning in memory or file writes to new locations.

Log Sources

Mutable Elements

Field	Description
UserContext	Filter by users with elevated privileges or service accounts
TimeWindow	Correlate access to .bash_history within X seconds of user switch or privilege escalation
ProcessNamePatterns	Add/remove CLI utilities used to read bash history

AN1086

A process or terminal command outside of standard shell utilities reads the user's .bash_history file. On macOS, unified logs or telemetry tools like EndpointSecurity (ESF) may observe file read APIs or terminal process lineage that shows non-user-initiated access.

Log Sources

Mutable Elements

Field	Description
ParentProcessCheck	Scope access to .bash_history only if parent is not Terminal.app or bash/zsh
AccessFrequency	Raise priority if .bash_history is accessed multiple times in short window