Detection Strategy for Plist File Modification (T1647), Detection Strategy DET0109

Archived: 2026-04-05 17:51:17 UTC

AN0306

Monitor for unexpected modifications of plist files in persistence or configuration directories (e.g., ~/Library/LaunchAgents, ~/Library/Preferences, /Library/LaunchDaemons). Detect when modifications are followed by execution of new or unexpected binaries. Track use of utilities such as defaults, plutil, or text editors making changes to Info.plist files. Correlate file modifications with subsequent process launches or service starts that reference the altered plist.

Log Sources

Data Component	Name	Channel
File Modification (DC0061)	macos:unifiedlog	write: File modifications to *.plist within LaunchAgents, LaunchDaemons, Application Support, or Preferences directories
Process Creation (DC0032)	macos:unifiedlog	exec: Execution of defaults, plutil, or common editors (vim/nano) targeting plist files
Command Execution (DC0064)	macos:unifiedlog	exec: Invocation of /usr/bin/defaults write or /usr/bin/plutil modifying plist keys

Mutable Elements

Field	Description
MonitoredDirectories	Set of directories where plist modifications are considered suspicious (e.g., ~/Library/LaunchAgents, /Library/LaunchDaemons)
SuspiciousKeys	List of plist keys associated with evasion or persistence (e.g., LSUIElement, LSEnvironment, ProgramArguments)
TimeWindow	Temporal correlation window to link plist file modifications with subsequent suspicious process launches