Detection Strategy for T1547.015 – Login Items on macOS, Detection Strategy DET0121

Archived: 2026-04-05 16:57:26 UTC

AN0340

Creation or modification of Login Items using AppleScript or Service Management Framework. Detection focuses on file creation/modification of `backgrounditems.btm`, new executables in `Contents/Library/LoginItems/`, use of `SMLoginItemSetEnabled` API, or suspicious processes triggered post-login without user interaction. Behavioral pivot includes anomalous AppleEvents, suspicious parent-child process pairs, and login-triggered execution chains.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Post-login execution of unrecognized child process from launchd or loginwindow
File Modification (DC0061)	macos:unifiedlog	Modification of backgrounditems.btm or creation of LoginItems subdirectory in .app bundle
OS API Execution (DC0021)	macos:unifiedlog	Invocation of SMLoginItemSetEnabled by non-system or recently installed application
Script Execution (DC0029)	macos:unifiedlog	AppleScript creating login item via 'System Events' dictionary

Mutable Elements

Field	Description
TimeWindow	Correlate file and process activity within a defined interval post-login (e.g., 0–5 minutes)
UserContext	Distinguish between system users, interactive users, and daemon contexts
ExecutableAllowlist	Define known-good login items to suppress false positives
PathRegexExclusion	Exclude common enterprise paths (e.g., Jamf, MDM-managed apps)

Source: https://attack.mitre.org/detectionstrategies/DET0121#AN0340