Detect Shell Configuration Modification for Persistence via Event-Triggered Execution, Detection Strategy DET0020

Archived: 2026-04-05 18:19:55 UTC

AN0059

Detects modification of shell startup/logout scripts such as ~/.bashrc, ~/.bash_profile, or /etc/profile, followed by anomalous process execution or network connections upon interactive or remote shell login.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines how soon after shell startup process execution or network activity is considered suspicious.
TargetUser	Limits detection to specific user accounts or roles such as root or service accounts.
FilePathRegex	Defines what shell configuration paths are considered relevant (e.g., .bashrc, .bash_logout, etc.)

AN0060

Correlates zsh shell configuration file changes (e.g., ~/.zshrc, ~/.zlogin, /etc/zprofile) with execution of unauthorized binaries or unexpected network activity triggered on Terminal.app launch.

Log Sources

Mutable Elements

Field	Description
FileTargetList	Customizable list of shell config files considered sensitive for detection.
PayloadEntropyThreshold	Used to distinguish benign from potentially obfuscated commands written to config files.
UserContext	Scoping based on user login class, e.g., administrative vs standard users.

Source: https://attack.mitre.org/detectionstrategies/DET0020