Detection Strategy for Boot or Logon Initialization Scripts: RC Scripts, Detection Strategy DET0237

Archived: 2026-04-05 12:53:14 UTC

AN0658

Detection of modified or newly created /etc/rc.local or /etc/init.d scripts followed by suspicious execution during system startup.

Log Sources

Mutable Elements

Field	Description
script_path	Specific path of init script (e.g., /etc/rc.local, /etc/init.d/*) may vary by distribution
user_context	Root vs. non-root modification context depending on configuration
time_window	Tuning window for script creation or modification relative to system boot

AN0659

Detection of edits or additions to /etc/rc.common, /Library/StartupItems, or /System/Library/StartupItems and associated script execution during login or reboot.

Log Sources

Mutable Elements

Field	Description
script_name	Name of script or LaunchDaemon plist is tunable across environments
event_interval	Time window between modification and reboot/login
file_permission	Permissions on modified RC files can vary between systems

AN0660

Detection of changes to /etc/rc.local.d/local.sh or rc.local during post-boot script execution with abnormal commands or additions.

Log Sources

Mutable Elements

Field	Description
script_section	Tunable script section edited by adversary (beginning, end, inline)
command_type	Nature of embedded command or payload affects detection scope
execution_trigger	Boot vs. manual script re-invocation

AN0661

Detection of modified boot-time configuration scripts that persist malicious CLI commands across reboots.

Log Sources

Mutable Elements

Field	Description
firmware_family	Device type or OS determines specific init script location
config_line_pattern	Regex or pattern matching approach to detect suspicious CLI
reboot_time_window	Time window between config change and first boot post-modification

---