Indicator Removal: Clear Linux or Mac System Logs, Sub-technique T1070.002 - Enterprise

Archived: 2026-04-05 17:24:10 UTC

Adversaries may clear system logs to hide evidence of an intrusion. macOS and Linux both keep track of system or user-initiated actions via system logs. The majority of native system logging is stored under the `/var/log/` directory. Subfolders in this directory categorize logs by their related functions, such as:[1]

- `/var/log/messages:` : General and system-related messages
- `/var/log/secure` or `/var/log/auth.log` : Authentication logs
- `/var/log/utmp` or `/var/log/wtmp` : Login records
- `/var/log/kern.log` : Kernel logs
- `/var/log/cron.log` : Crond logs
- `/var/log/maillog` : Mail server logs
- `/var/log/httpd/` : Web server access and error logs

Source: https://attack.mitre.org/techniques/T1070/002