# TTP Detail – T1070.002

## TTP Information

Name: Clear Linux or Mac System Logs

Description: 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 <code>/var/log/</code> directory. Subfolders in this directory categorize logs by their related functions, such as:(Citation: Linux Logs)

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

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* JumbledPath
* MacMa
* Proton
* UPSTYLE

## APTs (Intrusion Sets)

* Rocke
* Salt Typhoon
* Sea Turtle
* TeamTNT