ID: 513239
Sample Name: SZAYTvvY9Y
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:34:08
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

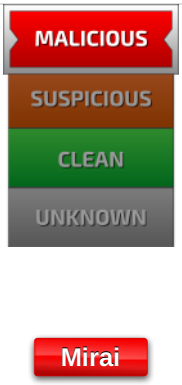
Linux Analysis Report SZAYTvvY9Y

Overview

General Information

Sample Name:	SZAYTvvY9Y
Analysis ID:	513239
MD5:	f274fb7e2b929c4..
SHA1:	a0285f5e70c6dc9..
SHA256:	6708e5ebbe503d..
Tags:	32 elf mips mirai
Infos:	

Detection

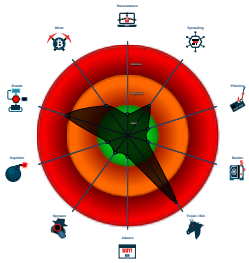


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Sample tries to persist itself using .d...
- Sample deletes itself
- Reads system files that contain reco...
- Uses known network protocols on no...
- Sample reads /proc/mounts (often u...
- Reads CPU information from /sys in...
- Yara signature match
- Writes Python files to disk

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

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:	513239
Start date:	01.11.2021
Start time:	23:34:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SZAYTvvY9Y
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.troj.evad.lin@0/112@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- SZAYTvvY9Y (PID: 5243, Parent: 5112, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/SZAYTvvY9Y
  - SZAYTvvY9Y New Fork (PID: 5247, Parent: 5243)
  - SZAYTvvY9Y New Fork (PID: 5248, Parent: 5243)
  - SZAYTvvY9Y New Fork (PID: 5250, Parent: 5243)
- systemd New Fork (PID: 5255, Parent: 1)
- journalctl (PID: 5255, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var

- systemd New Fork (PID: 5275, Parent: 1)
  - systemd-journald (PID: 5275, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5280, Parent: 1)
  - journalctl (PID: 5280, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- gdm3 New Fork (PID: 5324, Parent: 1320)
  - Default (PID: 5324, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5342, Parent: 1320)
  - Default (PID: 5342, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- dash New Fork (PID: 5343, Parent: 5113)
  - xdotool (PID: 5343, Parent: 5113, MD5: 38ea1b4bfcc631da4576723b24e1510e) Arguments: xdotool windowminimize
- python2.7 New Fork (PID: 5344, Parent: 4485)
  - srm (PID: 5344, Parent: 4485, MD5: 5d0db044b173f989a73a0790b19e79fa) Arguments: srm -fr /var/jbxkick /var/jbxinit.linux.py /home/saturnino/.config/autostart/jbxkick.desktop
- python2.7 New Fork (PID: 5347, Parent: 4485)
  - rm (PID: 5347, Parent: 4485, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -fr /var/jbxkick /var/jbxinit.linux.py /home/saturnino/.config/autostart/jbxkick.desktop
- python2.7 New Fork (PID: 5348, Parent: 2258)
  - umount (PID: 5348, Parent: 2258, MD5: 2a1758ef6cf863f285bc8a918edbc0be) Arguments: umount -v /var/jbxall
- udisksd New Fork (PID: 5371, Parent: 799)
  - dumpe2fs (PID: 5371, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/sda2
- udisksd New Fork (PID: 5373, Parent: 799)
  - dumpe2fs (PID: 5373, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- systemd New Fork (PID: 5378, Parent: 1860)
  - pulseaudio (PID: 5378, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5385, Parent: 1)
  - accounts-daemon (PID: 5385, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5400, Parent: 5385)
    - language-validate (PID: 5400, Parent: 5385, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
      - language-validate New Fork (PID: 5401, Parent: 5400)
      - language-options (PID: 5401, Parent: 5400, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
        - language-options New Fork (PID: 5402, Parent: 5401)
        - sh (PID: 5402, Parent: 5401, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
          - sh New Fork (PID: 5403, Parent: 5402)
          - locale (PID: 5403, Parent: 5402, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
          - sh New Fork (PID: 5404, Parent: 5402)
          - grep (PID: 5404, Parent: 5402, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm-session-worker New Fork (PID: 5386, Parent: 1809)
  - Default (PID: 5386, Parent: 1809, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PostSession/Default
- gdm3 New Fork (PID: 5405, Parent: 1320)
  - gdm-session-worker (PID: 5405, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5422, Parent: 5405)
    - gdm-wayland-session (PID: 5422, Parent: 5405, 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: 5425, Parent: 5422)
      - dbus-run-session (PID: 5425, Parent: 5422, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5426, Parent: 5425)
        - dbus-daemon (PID: 5426, Parent: 5425, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
          - dbus-daemon New Fork (PID: 5430, Parent: 5426)
            - dbus-daemon New Fork (PID: 5431, Parent: 5430)
            - false (PID: 5431, Parent: 5430, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5433, Parent: 5426)
            - dbus-daemon New Fork (PID: 5434, Parent: 5433)
            - false (PID: 5434, Parent: 5433, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5435, Parent: 5426)
            - dbus-daemon New Fork (PID: 5436, Parent: 5435)
            - false (PID: 5436, Parent: 5435, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5437, Parent: 5426)
            - dbus-daemon New Fork (PID: 5438, Parent: 5437)
            - false (PID: 5438, Parent: 5437, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5439, Parent: 5426)
            - dbus-daemon New Fork (PID: 5440, Parent: 5439)
            - false (PID: 5440, Parent: 5439, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5441, Parent: 5426)
            - dbus-daemon New Fork (PID: 5442, Parent: 5441)
            - false (PID: 5442, Parent: 5441, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5444, Parent: 5426)
            - dbus-daemon New Fork (PID: 5445, Parent: 5444)
            - false (PID: 5445, Parent: 5444, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-run-session New Fork (PID: 5427, Parent: 5425)
        - gnome-session (PID: 5427, Parent: 5425, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary (PID: 5427, Parent: 5425, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
          - gnome-session-binary New Fork (PID: 5446, Parent: 5427)
          - session-migration (PID: 5446, Parent: 5427, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
          - gnome-session-binary New Fork (PID: 5447, Parent: 5427)
          - sh (PID: 5447, Parent: 5427, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
          - gnome-shell (PID: 5447, Parent: 5427, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5416, Parent: 1320)
  - Default (PID: 5416, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5473, Parent: 1320)
  - gdm-session-worker (PID: 5473, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5490, Parent: 5473)
    - gdm-x-session (PID: 5490, Parent: 5473, MD5: 498a824333f1c1ec7767f4612d1887cc) Arguments: /usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
      - gdm-x-session New Fork (PID: 5494, Parent: 5490)
      - Xorg (PID: 5494, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg.wrap (PID: 5494, Parent: 5490, MD5: 48993830888200ecf19dd7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg (PID: 5494, Parent: 5490, MD5: 730cf4c45a7ee8bea88abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none

-noreset -keeptty -verbose 3
- Xorg New Fork (PID: 5506, Parent: 5494)
- sh (PID: 5506, Parent: 5494, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
  - sh New Fork (PID: 5507, Parent: 5506)
  - xkbcomp (PID: 5507, Parent: 5506, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
- Xorg New Fork (PID: 5752, Parent: 5494)
- sh (PID: 5752, Parent: 5494, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
  - sh New Fork (PID: 5753, Parent: 5752)
  - xkbcomp (PID: 5753, Parent: 5752, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm

- gdm-x-session New Fork (PID: 5512, Parent: 5490)
- Default (PID: 5512, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
- gdm-x-session New Fork (PID: 5513, Parent: 5490)
- dbus-run-session (PID: 5513, Parent: 5490, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
  - dbus-run-session New Fork (PID: 5514, Parent: 5513)
  - dbus-daemon (PID: 5514, Parent: 5513, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
    - dbus-daemon New Fork (PID: 5529, Parent: 5514)
      - dbus-daemon New Fork (PID: 5530, Parent: 5529)
      - at-spi-bus-launcher (PID: 5530, Parent: 5529, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
        - at-spi-bus-launcher New Fork (PID: 5535, Parent: 5530)
        - dbus-daemon (PID: 5535, Parent: 5530, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
          - dbus-daemon New Fork (PID: 5867, Parent: 5535)
            - dbus-daemon New Fork (PID: 5868, Parent: 5867)
            - at-spi2-registryd (PID: 5868, Parent: 5867, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
    - dbus-daemon New Fork (PID: 5559, Parent: 5514)
      - dbus-daemon New Fork (PID: 5560, Parent: 5559)
      - false (PID: 5560, Parent: 5559, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5562, Parent: 5514)
      - dbus-daemon New Fork (PID: 5563, Parent: 5562)
      - false (PID: 5563, Parent: 5562, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5564, Parent: 5514)
      - dbus-daemon New Fork (PID: 5565, Parent: 5564)
      - false (PID: 5565, Parent: 5564, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5566, Parent: 5514)
      - dbus-daemon New Fork (PID: 5567, Parent: 5566)
      - false (PID: 5567, Parent: 5566, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5568, Parent: 5514)
      - dbus-daemon New Fork (PID: 5569, Parent: 5568)
      - false (PID: 5569, Parent: 5568, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5570, Parent: 5514)
      - dbus-daemon New Fork (PID: 5571, Parent: 5570)
      - false (PID: 5571, Parent: 5570, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5573, Parent: 5514)
      - dbus-daemon New Fork (PID: 5574, Parent: 5573)
      - false (PID: 5574, Parent: 5573, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5750, Parent: 5514)
      - dbus-daemon New Fork (PID: 5751, Parent: 5750)
      - ibus-portal (PID: 5751, Parent: 5750, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
    - dbus-daemon New Fork (PID: 5874, Parent: 5514)
      - dbus-daemon New Fork (PID: 5875, Parent: 5874)
      - gjs (PID: 5875, Parent: 5874, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
    - dbus-daemon New Fork (PID: 5936, Parent: 5514)
      - dbus-daemon New Fork (PID: 5937, Parent: 5936)
      - false (PID: 5937, Parent: 5936, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-run-session New Fork (PID: 5515, Parent: 5513)
  - gnome-session (PID: 5515, Parent: 5513, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
  - gnome-session-binary (PID: 5515, Parent: 5513, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
    - gnome-session-binary New Fork (PID: 5516, Parent: 5515)
    - gnome-session-check-accelerated (PID: 5516, Parent: 5515, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
      - gnome-session-check-accelerated New Fork (PID: 5536, Parent: 5516)
      - gnome-session-check-accelerated-gl-helper (PID: 5536, Parent: 5516, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
      - gnome-session-check-accelerated New Fork (PID: 5548, Parent: 5516)
      - gnome-session-check-accelerated-gles-helper (PID: 5548, Parent: 5516, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
    - gnome-session-binary New Fork (PID: 5575, Parent: 5515)
    - session-migration (PID: 5575, Parent: 5515, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
    - gnome-session-binary New Fork (PID: 5576, Parent: 5515)
    - sh (PID: 5576, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
    - gnome-shell (PID: 5576, Parent: 5515, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
      - gnome-shell New Fork (PID: 5623, Parent: 5576)
      - ibus-daemon (PID: 5623, Parent: 5576, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
        - ibus-daemon New Fork (PID: 5746, Parent: 5623)
        - ibus-memconf (PID: 5746, Parent: 5623, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
        - ibus-daemon New Fork (PID: 5748, Parent: 5623)
          - ibus-daemon New Fork (PID: 5749, Parent: 5748)
          - ibus-x11 (PID: 5749, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
        - ibus-daemon New Fork (PID: 5915, Parent: 5623)
        - ibus-engine-simple (PID: 5915, Parent: 5623, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
    - gnome-session-binary New Fork (PID: 5890, Parent: 5515)
    - sh (PID: 5890, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
    - gsd-sharing (PID: 5890, Parent: 5515, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing

- gnome-session-binary New Fork (PID: 5892, Parent: 5515)
  - sh (PID: 5892, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
  - gsd-wacom (PID: 5892, Parent: 5515, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 5894, Parent: 5515)
  - sh (PID: 5894, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
  - gsd-color (PID: 5894, Parent: 5515, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 5895, Parent: 5515)
  - sh (PID: 5895, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
  - gsd-keyboard (PID: 5895, Parent: 5515, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 5896, Parent: 5515)
  - sh (PID: 5896, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 5896, Parent: 5515, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6090, Parent: 5896)
      - gsd-print-notifications New Fork (PID: 6091, Parent: 6090)
      - gsd-printer (PID: 6091, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 5897, Parent: 5515)
  - sh (PID: 5897, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
  - gsd-rfkill (PID: 5897, Parent: 5515, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 5898, Parent: 5515)
  - sh (PID: 5898, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
  - gsd-smartcard (PID: 5898, Parent: 5515, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 5899, Parent: 5515)
  - sh (PID: 5899, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
  - gsd-datetime (PID: 5899, Parent: 5515, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 5903, Parent: 5515)
  - sh (PID: 5903, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
  - gsd-media-keys (PID: 5903, Parent: 5515, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 5904, Parent: 5515)
  - sh (PID: 5904, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
  - gsd-screensaver-proxy (PID: 5904, Parent: 5515, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 5905, Parent: 5515)
  - sh (PID: 5905, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
  - gsd-sound (PID: 5905, Parent: 5515, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 5909, Parent: 5515)
  - sh (PID: 5909, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
  - gsd-a11y-settings (PID: 5909, Parent: 5515, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 5911, Parent: 5515)
  - sh (PID: 5911, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
  - gsd-housekeeping (PID: 5911, Parent: 5515, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 5914, Parent: 5515)
  - sh (PID: 5914, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
  - gsd-power (PID: 5914, Parent: 5515, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6417, Parent: 5515)
  - sh (PID: 6417, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
  - spice-vdagent (PID: 6417, Parent: 5515, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 6419, Parent: 5515)
  - sh (PID: 6419, Parent: 5515, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
  - xbrlapi (PID: 6419, Parent: 5515, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q
- gdm3 New Fork (PID: 5474, Parent: 1320)
  - Default (PID: 5474, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5475, Parent: 1320)
  - Default (PID: 5475, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gvfsd-fuse New Fork (PID: 5479, Parent: 2038)
  - fusermount (PID: 5479, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5491, Parent: 1)
  - systemd-user-runtime-dir (PID: 5491, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5600, Parent: 1)
  - systemd-localed (PID: 5600, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5761, Parent: 1334)
  - pulseaudio (PID: 5761, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5764, Parent: 1)
  - geoclue (PID: 5764, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 5940, Parent: 1)
  - systemd-hostnamed (PID: 5940, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6175, Parent: 1)
  - systemd-localed (PID: 6175, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 6302, Parent: 1)
  - fprintd (PID: 6302, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SZAYTvvY9Y	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x168c4:$xo1: \x175 366;uotj • 0x16934:$xo1: \x175 366;uotj • 0x169a4:$xo1: \x175 366;uotj • 0x16a14:$xo1: \x175 366;uotj • 0x16a84:$xo1: \x175 366;uotj
SZAYTvvY9Y	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x16480:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
SZAYTvvY9Y	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

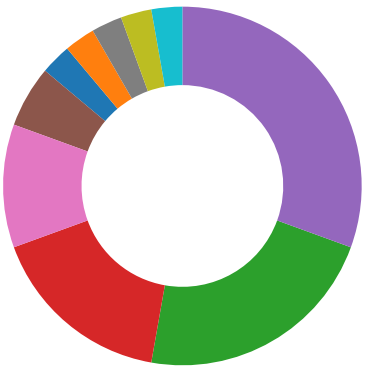
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5243.1.0000000060ca3480.0000000056a06d25.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x2284:$xo1: \x175 366;uotj • 0x22f8:$xo1: \x175 366;uotj • 0x236c:$xo1: \x175 366;uotj • 0x23e0:$xo1: \x175 366;uotj • 0x2454:$xo1: \x175 366;uotj
5247.1.000000003025a7fd.00000000e5ff32fb.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x168c4:$xo1: \x175 366;uotj • 0x16934:$xo1: \x175 366;uotj • 0x169a4:$xo1: \x175 366;uotj • 0x16a14:$xo1: \x175 366;uotj • 0x16a84:$xo1: \x175 366;uotj
5247.1.000000003025a7fd.00000000e5ff32fb.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x16480:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
5247.1.000000003025a7fd.00000000e5ff32fb.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5250.1.0000000060ca3480.0000000056a06d25.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x2284:$xo1: \x175 366;uotj • 0x22f8:$xo1: \x175 366;uotj • 0x236c:$xo1: \x175 366;uotj • 0x23e0:$xo1: \x175 366;uotj • 0x2454:$xo1: \x175 366;uotj
Click to see the 11 entries				

Jbx Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

Uses known network protocols on non-standard ports

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Sample tries to persist itself using .desktop files

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

Hooking and other Techniques for Hiding and Protection:

Sample deletes itself

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

Remote Access Functionality:

Yara detected Mirai

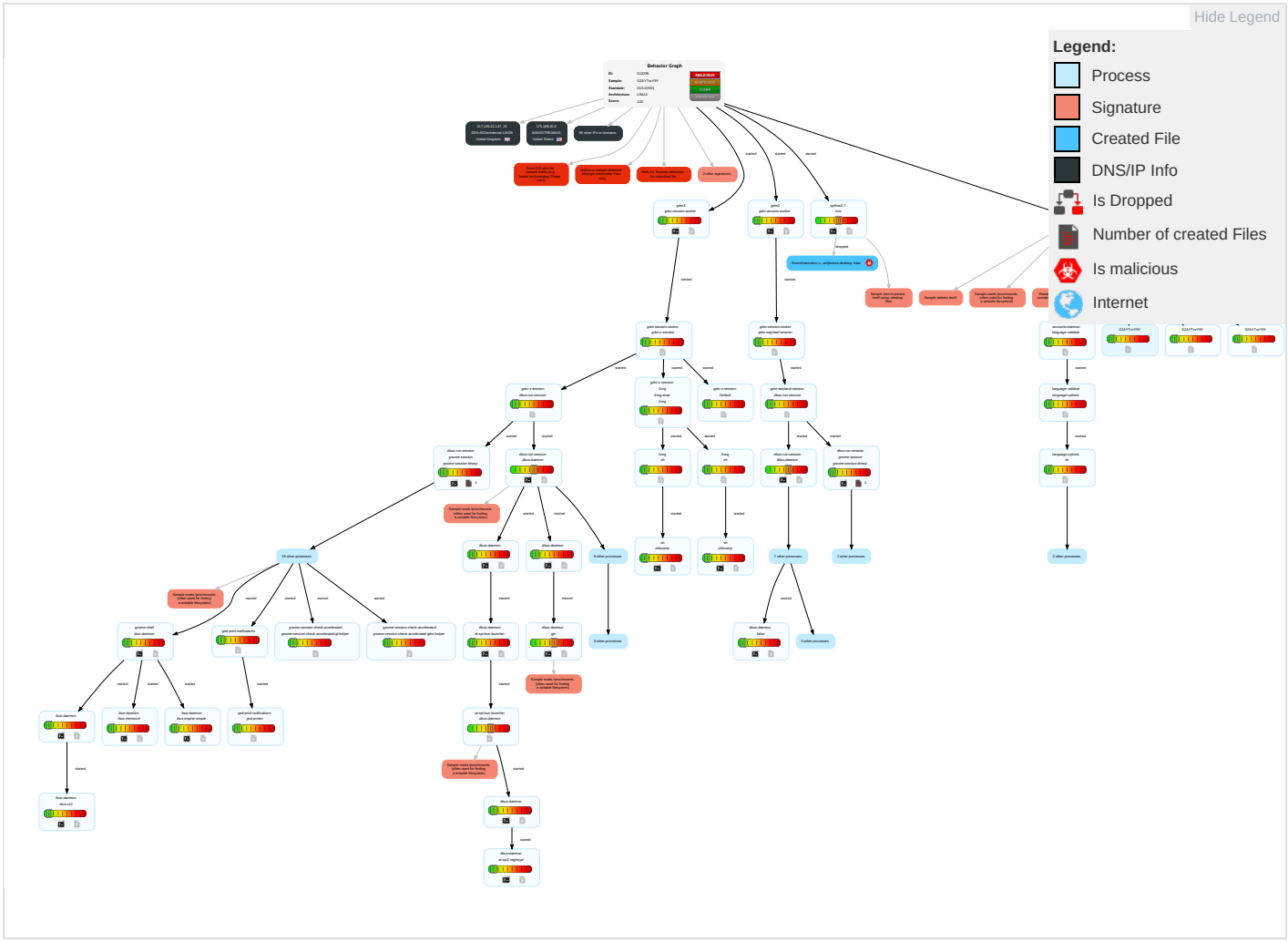
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Imp
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Scheduled Task/Job 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	Mod Sys Par
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 2	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	Dev Loc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Del Dev Dat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Indicator Removal on Host 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Car Billi Frau
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Mar App Ran or F

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SZAYTvvY9Y	38%	Virustotal		Browse
SZAYTvvY9Y	55%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.114.175.86	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
9.207.27.19	unknown	United States		3356	LEVEL3US	false
69.142.48.73	unknown	United States		7922	COMCAST-7922US	false
146.26.119.14	unknown	United States		197938	TRAVIANGAMESDE	false
104.15.73.51	unknown	United States		7018	ATT-INTERNET4US	false
195.10.52.220	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
186.56.181.240	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
218.215.222.106	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	false
209.123.159.201	unknown	United States		8001	NET-ACCESS-CORPUS	false
169.192.248.17	unknown	United States		37611	AfrihostZA	false
53.139.99.46	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
25.140.116.154	unknown	United Kingdom		7922	COMCAST-7922US	false
197.3.63.189	unknown	Tunisia		37705	TOPNETTN	false
80.250.244.54	unknown	Slovakia (SLOVAK Republic)		5578	AS-BENESTRABratislavaSlovakRepublicSK	false
5.236.134.237	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
170.155.48.13	unknown	Argentina		27967	GobernaciondelaProvinciadeBuenosAiresAR	false
34.173.106.181	unknown	United States		2686	ATGS-MMD-ASUS	false
150.240.17.42	unknown	United States		1479	DNIC-ASBLK-01478-01479US	false
88.52.104.178	unknown	Italy		3269	ASN-IBSNAZIT	false
95.76.26.248	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
75.177.252.219	unknown	United States		11426	TWC-11426-CAROLINASUS	false
220.246.216.123	unknown	Hong Kong		4760	HKTIMS-APHKTLimitedHK	false
14.171.11.141	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
135.93.130.159	unknown	United States		10455	LUCENT-CIOUS	false
34.11.101.203	unknown	United States		2686	ATGS-MMD-ASUS	false
118.48.111.61	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
95.6.137.33	unknown	Turkey		9121	TTNETTR	false
217.155.41.147	unknown	United Kingdom		13037	ZEN-ASZenInternet-UKGB	false
83.106.12.197	unknown	United Kingdom		2529	DEMON-INTERNETNowmaintainedbyCableWirelessWorldwide	false
80.108.189.170	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
108.13.86.230	unknown	United States		5650	FRONTIER-FRTRUS	false
161.247.27.64	unknown	United States		26539	GIANT-FOOD-INCUS	false
217.162.249.202	unknown	Switzerland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
132.214.230.219	unknown	Canada		33602	TELUQCA	false
34.81.11.77	unknown	United States		15169	GOOGLEUS	false
206.33.185.11	unknown	United States		3356	LEVEL3US	false
72.67.239.16	unknown	United States		5650	FRONTIER-FRTRUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
120.150.226.5	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
137.250.128.90	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
139.8.196.153	unknown	Germany		9905	LINKNET-ID-APLinknetASNID	false
142.219.199.121	unknown	Canada		53442	CITY-OF-COQUITLAMCA	false
48.88.173.154	unknown	United States		2686	ATGS-MMD-ASUS	false
128.18.204.181	unknown	United States		264	SRINET-ASUS	false
77.60.19.67	unknown	Netherlands		1136	KPNKPNNationalEU	false
119.48.25.145	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
32.71.25.105	unknown	United States		2686	ATGS-MMD-ASUS	false
188.160.154.140	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
88.73.217.63	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
182.0.0.137	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
2.222.184.187	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
220.161.193.24	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
34.45.16.132	unknown	United States		2686	ATGS-MMD-ASUS	false
80.122.167.237	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
108.194.245.80	unknown	United States		7018	ATT-INTERNET4US	false
117.11.224.254	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
111.63.96.99	unknown	China		24547	CMNET-V4HEBEI-AS-APHebeiMobileCommunicationCompanyLimit	false
173.124.66.194	unknown	United States		10507	SPCSUS	false
220.161.2.122	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
20.74.1.43	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
183.62.106.32	unknown	China		4816	CHINANET-IDC-GDChinaTelecomGroupCN	false
9.55.228.101	unknown	United States		3356	LEVEL3US	false
157.213.201.203	unknown	United States		4704	SANNETRakutenMobileIncJP	false
173.188.30.6	unknown	United States		7029	WINDSTREAMUS	false
88.41.34.69	unknown	Italy		3269	ASN-IBSNAZIT	false
118.140.192.85	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
145.233.36.105	unknown	United Kingdom		3549	LVLT-3549US	false
145.4.3.12	unknown	Netherlands		702	UUNETUS	false
218.124.61.47	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
146.74.25.222	unknown	United States		30051	SCCGOVUS	false
4.93.103.173	unknown	United States		3356	LEVEL3US	false
141.200.191.152	unknown	Germany		41587	ATLAS-ELEKTRONIKSebaldsbrueckerHeerstrasse235DE	false
121.226.187.124	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
123.211.111.178	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
182.8.245.166	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
188.242.132.208	unknown	Russian Federation		35807	SKYNET-SPB-ASRU	false
77.145.164.187	unknown	France		15557	LDCOMNETFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.187.247.165	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
41.216.51.182	unknown	Benin		28683	BENINTELECOMBJ	false
126.28.125.143	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
121.170.84.79	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
37.223.25.192	unknown	Spain		12430	VODAFONE_ESES	false
154.134.179.153	unknown	Egypt		37069	MOBINILEG	false
53.20.182.103	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
14.36.212.117	unknown	Korea Republic of		18032	SHINHANSYS-AS-KRSHINHANDSKR	false
152.131.33.86	unknown	United States		29992	VA-TMP-COREUS	false
5.214.242.236	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
18.251.67.211	unknown	United States		16509	AMAZON-02US	false
27.6.83.212	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	false
25.138.160.44	unknown	United Kingdom		7922	COMCAST-7922US	false
53.92.73.63	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
79.188.24.154	unknown	Poland		5617	TPNETPL	false
123.36.202.109	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
132.170.28.40	unknown	United States		7939	UNIVCENTFLAUS	false
175.94.80.106	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
171.6.101.90	unknown	Thailand		45758	TRIPLETNET-AS-APTripleTInternetTripleTBroadbandTH	false
38.16.79.218	unknown	United States		174	COGENT-174US	false
54.254.156.131	unknown	United States		16509	AMAZON-02US	false
133.74.96.232	unknown	Japan		3488	JAXANETInformationSystemsDepartmentJapanAerospaceExpl	false
65.3.68.26	unknown	United States		16509	AMAZON-02US	false
101.166.215.220	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.11.101.203	u9afRawaNV	Get hash	malicious	Browse	
47.114.175.86	DEMONS.x86	Get hash	malicious	Browse	
217.155.41.147	DEMONS.arm7	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	ENYxttDmO1	Get hash	malicious	Browse	• 8.158.74.46
	1Y2rsDBP9s	Get hash	malicious	Browse	• 47.107.186.73
	Ko84iLip1u	Get hash	malicious	Browse	• 120.26.45.127
	t7WU0JjLAR	Get hash	malicious	Browse	• 8.173.77.186
	izTs48VpFZ	Get hash	malicious	Browse	• 47.113.156.12
	I5A5LzSAql	Get hash	malicious	Browse	• 47.119.119.166

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mipsel	Get hash	malicious	Browse	• 8.151.21.111
	arm7-20211101-1513	Get hash	malicious	Browse	• 101.37.208.244
	mxHkqAIYT0	Get hash	malicious	Browse	• 8.168.141.85
	swOGb2sZYt	Get hash	malicious	Browse	• 8.139.185.129
	sStP2Druko.exe	Get hash	malicious	Browse	• 121.199.35.188
	9o6Z1wEokT	Get hash	malicious	Browse	• 47.105.148.45
	yxD7DmfG2j	Get hash	malicious	Browse	• 8.169.211.147
	pTF1ilCUEm	Get hash	malicious	Browse	• 39.96.157.236
	032k4JmR0U	Get hash	malicious	Browse	• 42.120.76.137
	x86	Get hash	malicious	Browse	• 115.28.63.138
	z0x3n.x86	Get hash	malicious	Browse	• 8.166.90.215
	z0x3n.arm	Get hash	malicious	Browse	• 121.40.4.13
	arm	Get hash	malicious	Browse	• 47.120.104.131
	T0uznhDXKw	Get hash	malicious	Browse	• 121.41.250.157
LEVEL3US	ENYxttDmO1	Get hash	malicious	Browse	• 9.211.168.143
	7DoAjWX5uZ	Get hash	malicious	Browse	• 8.90.169.244
	1Y2rsDBP9s	Get hash	malicious	Browse	• 9.152.224.236
	Ko84iLip1u	Get hash	malicious	Browse	• 9.241.163.111
	arH2Af5qoc	Get hash	malicious	Browse	• 205.131.54.153
	t7WU0JjLAR	Get hash	malicious	Browse	• 216.202.137.30
	FGVOkw9did	Get hash	malicious	Browse	• 9.152.184.121
	u4M7XeqKtD	Get hash	malicious	Browse	• 9.33.31.156
	Yoshi.arm7	Get hash	malicious	Browse	• 209.4.249.91
	Yoshi.x86	Get hash	malicious	Browse	• 4.255.186.89
	Yoshi.arm	Get hash	malicious	Browse	• 4.230.207.8
	mipsel	Get hash	malicious	Browse	• 4.156.52.193
	arm	Get hash	malicious	Browse	• 9.23.178.145
	arm7-20211101-1513	Get hash	malicious	Browse	• 4.219.252.134
	JjHQ8Q1weT	Get hash	malicious	Browse	• 9.50.50.245
	anWxzNav9N	Get hash	malicious	Browse	• 4.41.252.215
	mxHkqAIYT0	Get hash	malicious	Browse	• 212.187.176.253
	Antisocial.x86	Get hash	malicious	Browse	• 192.91.253.232
	Antisocial.arm	Get hash	malicious	Browse	• 9.73.7.178
	swOGb2sZYt	Get hash	malicious	Browse	• 8.113.103.123
COMCAST-7922US	7DoAjWX5uZ	Get hash	malicious	Browse	• 96.201.85.34
	1Y2rsDBP9s	Get hash	malicious	Browse	• 73.105.107.74
	Ko84iLip1u	Get hash	malicious	Browse	• 73.105.10.74
	arH2Af5qoc	Get hash	malicious	Browse	• 174.176.37.163
	FGVOkw9did	Get hash	malicious	Browse	• 73.61.239.80
	izTs48VpFZ	Get hash	malicious	Browse	• 184.125.31.24
	I5A5LzSAql	Get hash	malicious	Browse	• 67.160.101.236
	P8AVd483d7	Get hash	malicious	Browse	• 96.193.105.162
	mRQwOz6Oit	Get hash	malicious	Browse	• 71.192.206.245
	u4M7XeqKtD	Get hash	malicious	Browse	• 68.63.192.0
	Yoshi.arm7	Get hash	malicious	Browse	• 96.110.194.148
	Yoshi.x86	Get hash	malicious	Browse	• 96.68.76.219
	Yoshi.arm	Get hash	malicious	Browse	• 76.105.89.111
	OdIBX0NYRS.dll	Get hash	malicious	Browse	• 50.243.30.51
	mipsel	Get hash	malicious	Browse	• 76.117.226.131
	arm7-20211101-1513	Get hash	malicious	Browse	• 73.134.196.246
	mips	Get hash	malicious	Browse	• 73.238.165.37
	anWxzNav9N	Get hash	malicious	Browse	• 96.124.240.74
	mxHkqAIYT0	Get hash	malicious	Browse	• 96.220.145.198
	Antisocial.arm	Get hash	malicious	Browse	• 185.102.172.132

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/home/saturnino/.config/autostart/jbxkick.desktop	
Process:	/usr/bin/srm
File Type:	data
Category:	dropped
Size (bytes):	1245222
Entropy (8bit):	6.0173905238453
Encrypted:	false
SSDEEP:	6144:835kqYtk/xASzVaO3UFaXDrzxVBC38tG5tbSk2t+FskmuVAG:NqYyZDoFaTxvCf5Mk2t+FTfL
MD5:	EDCEE8DB6B5E75FEAFD2C96C227235B3
SHA1:	0BD7F024C82EB15DD8CB267BFE33E8FF8EA412EF
SHA-256:	870E6B973C228D76CF8F498B57DFD3F9F7529F3AFA822709C1D7281E25FC536D
SHA-512:	D0D2C5BDA44A7BD6609BDA74D118F3C16F8BC6B1F5BF8589FE093196335F034C5B4C2A46D611ABE25651A28CF084D6149C1A34645293E75C189A3B2146719D0
Malicious:	**true**
Reputation:	low
Preview:	....

/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/5431/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

/proc/5431/oom_score_adj	
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5434/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5436/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5438/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5440/oom_score_adj	
Process:	/usr/bin/dbus-daemon

/proc/5440/oom_score_adj	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5442/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5445/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/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
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5560/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5563/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5565/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5567/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5569/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5571/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5574/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5751/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5868/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5875/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5937/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/run/mount/utab.KpH2dA	
Process:	/usr/bin/umount
File Type:	ASCII text
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.061412716358383
Encrypted:	false
SSDEEP:	12:zBoMcjFyq+tMNjFydUtMbfjFys2MfjFyR4MljFyf0MXgjFyZMbUjF3AbXOTQXgIh:+FyqrFydUALFyspFyjFyjAFys0FQbXOK
MD5:	4B58EC063938B7815DF01A90F41378FD
SHA1:	E27B39B7B7DF22F1547CAD0E1940DEC7B88BCC14
SHA-256:	0FBA06A3E816BF5EE615EDC9BAAF72FD36C2ACB14C1D8C14CEF04815C4FC82E3
SHA-512:	1FE25D45EF301F6221C2E3317E09B250D16CFBBC398417D149B107284DCC00418C8AC7623AED60D7087A11AB5D90F690D9CACC7B0EDA7943CA4E03FB18325F 5
Malicious:	false

/run/mount/utab.KpH2dA	
Preview:	SRC=/dev/loop0 TARGET=/snap/core18/2128 ROOT=/ OPTS=x-gdu.hide.SRC=/dev/loop3 TARGET=/snap/snapd/12704 ROOT=/ OPTS=x-gdu.hide.SRC=/dev/loop2 TARGET=/snap/lxd/21029 ROOT=/ OPTS=x-gdu.hide.SRC=/dev/loop1 TARGET=/snap/core18/1944 ROOT=/ OPTS=x-gdu.hide.SRC=/dev/loop6 TARGET=/snap/snapd/12883 ROOT=/ OPTS=x-gdu.hide.SRC=/dev/loop4 TARGET=/snap/core20/1081 ROOT=/ OPTS=x-gdu.hide.SRC=/dev/loop7 TARGET=/snap/lxd/21545 ROOT=/ OPTS=x-gdu.hide.SRC=//192.168.2.1/esxi07-Ubuntu20 TARGET=/var/jbxanalysis ROOT=/ OPTS=user=guest.

/run/systemd/journal/streams/.#9:74061FwvVq3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.511506653322648
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8FaO9EWWsjs7Lbgw3:SbFuFyLVIg1BG+f+M8Fa8jji4s
MD5:	35B77FDA7EFE5F08F923492C87CB402D
SHA1:	086862CBC39F7A6E553268A219284CE13694FA46
SHA-256:	F74CDBEE31A54092DBD11E30DD2AB1FF502129187E9289693E029B45919B9D61
SHA-512:	89BEDD5626BFB7549CB540A641C2137D8C692D9886B1308FAA7EC0C935FF55BC83E973C89DB18188ED5F4A5D20BE17107316B6B9929D7DD8001E074365CD6A(
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=608cd20eb7bf40dead50494f702a33f2.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:74062zCOWc6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.521849731737253
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M8UU3KZDEuvcTqji4s:qgFq6g10+f+M8AD4es
MD5:	4FABC8B80F7650DC937ABBB77102460F
SHA1:	7D7F593D37CE8B64D0FCD91B060822341318EA99
SHA-256:	0D1D9961BCBA6910F934256C7C11097EDD20F9FF7407C7D014B96DFAC50DCBED
SHA-512:	F6F8E6FB9D120CA34DA3D4CE3D85EA5EED63E7E4ADD7C542EE301AE490E2FB3A948E410ECC37F0FAFA725959ABE6BBF2925147C2838E577FE9607033B6C2125
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=6cf130a76dc741d69fbc2d0abf698bc9.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:74374Zmrke6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.3507876845105535
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm9bRyEGBALGAFoRxsh:SbFuFyLVIg1BG+f+MFRXGBgGaoRqjtWQ
MD5:	643E654E165E4C46AF8597AFED2EA93B
SHA1:	B82749EC0C174DC7F13E9704AF421E3F64FF7B3A
SHA-256:	8E72FEB0B35EBEB6098FC119C7691F548AE7C1B394B6AFD918EE2FD7DB711A70
SHA-512:	FE2044593698BF29069FDE5E48F0878F93D5C4C445C9C161A0C1FCD7EC3874F718E715A3CE3801CBAEEE6CB6DB0FF1384BCCC17DEADF10BCB9E5A8AC664B1121
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=75d6e6c423314f4c96eacdef2ce55933.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:744602mcqA5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.432096818957463
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MNBFQTuqjLTTIWTIL:qgFq6g10+f+MNTuu+EWEL
MD5:	E962A8AB305ED15C18ED110EDAC508B6

/run/systemd/journal/streams/.#9:744602mcqA5	
SHA1:	DD455D5E25344996CDA3BDD52DFCBE249C2CC269
SHA-256:	B1EF1DBC55FC6732E68BF9611777D746F849760DE3020C9D7E65074F4CA94E2A
SHA-512:	11D92B37725902FC848EFEE9BEFA154D4AE49138290778A2C9903E8BE5C654D27EDD6B3DC0992133475AF66D08AD826F7AAC1650F05F8369D70F4A7E88F2385F
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=cf0f407ce6504d55a0177f2549984191.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service.

/run/systemd/journal/streams/.#9:74665pyuJq3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.393823822229638
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmo8dsHqaB7sjs2BI:SbFuFyLVK6g7/+BG+f+Mo8dJaBojNq
MD5:	75F669DE33930424964688F8061F2DBB
SHA1:	E37314E12F7D328E81790485ADFCFA90ED35744D
SHA-256:	C4DC063D013FBF652158B19F3746CD59508020C27C1BD6C698431A68EE01A5B4
SHA-512:	2373745E9BDA4B6C1F64F0F264510E98FAF476B3F2CFB4F3F3D650E62282120A4816667C53FCE9E7A784E7835D93C511DC06B9835D0DC785BC72D505C2BD3DA
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=b0382dce3baf4b85b5ac37d5d3a2db73.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:74666fOFZU3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.374202793466853
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm+tRRzgt4ly2Auxb:SbFuFyLVI6g7/+BG+f+M+tXkSY2RqjNq
MD5:	F7C2E50A846A31644F23E091389D091A
SHA1:	A53AFF2214CB31ABC7AE464A015BEE4403AA29F1
SHA-256:	1FA71EFF1370EB1D29358A1C295E3D7033D11077FF1C066235A065B92682FE9A
SHA-512:	C3D566406C88B4711990A8195638ACFFEB6F4B52B385A59C0F116882D6C7A5B86AD2C3CE6D722C44C7A612933518DC64B0745A90E6A5ABF35751BA5440FFCCB
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=4acb7c4422b64cb7a7ba58d48ee85441.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:74732L9yIy5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.459924450466257
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M4E/wV2QwjFQMzKYA9:qgFqo6g7/+0+f+M4QTTmt9
MD5:	6B1316ABB13A4619FFF63F8F208F44E7
SHA1:	86349E0BF248FB62D449E88488B2D4A0C66439D5
SHA-256:	32B0290C27D45A81E381C4C4D25838FA7B72122E8A4794B1D115C66212A1E7B4
SHA-512:	8F213DA84FAC501EC95FF9119A4009EB15327AC14378FF0E83971BE8568E6B939D71EC052C6600298921CD2A786AB0391A80A7B1310B43A6CB72640B03945C1C
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=234ffa0c31174309bdd0c9a3a6aa372b.IDENTIFIER=/usr/lib/gdm3/gdm-x-session.

/run/systemd/journal/streams/.#9:74733Cdldh6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.490428462851178
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+Mxdq70jFQMzKYA9:qgFqdg7/+0+f+Mx0KTmt9

/run/systemd/journal/streams/.#9:74733Cdldh6	
MD5:	1D913BA33AF28864B10C954DF71C7CF7
SHA1:	FCF087B8713E30529FEFA7237735C38153DFC872
SHA-256:	BE2E4EDE9B07D4DE54DD01494C17403DE3E4BE71954A351938E52477CD2A3046
SHA-512:	48823592E5E33A2FED0EDFFD7BCC15A8B09E9F186B1030FE440C43E4BF149CC1CF65745FEC710135EE8A5E02A68DB33F526633B7ED349FE3013CB7E0DED308 4
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=9880c6a0dd694ad1bb732e756d4a8cc2.IDENTIFIER=/usr/lib/gdm3/gdm-x-session.

/run/systemd/journal/streams/.#9:747347bGeo4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.450267417773655
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MoBdtjZcHuWasl6m5esl61Udr+:qgFq6g10+f+MoBJmuWap6eep6eE
MD5:	0D68136658C3F40536A360F70E7F941F
SHA1:	FCC4AF94E93F1CE097870E0EA327F46F499DED72
SHA-256:	44E0BE158085838465902F560DCCB58CF737A4F7D0D4DE4B0240F792408B8E04
SHA-512:	D6F3D140409DED87EA96A8C6E3CD13E1EDECFA01BB9A88EA8752BD055DD08274CD01E877CD7032CF1CC533D8E16AE9BCDBA8F97A4CE0E43D9CA1A5E2ACC 1D0A7
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=bd3e2f3a45d14f6083ad90b44c54b8a1.IDENTIFIER=systemd-user-runtime-dir.UNIT=user-runtime-dir@1000.service.

/run/systemd/journal/streams/.#9:75370JwuCO4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.439744942446988
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm5yTEQXwvQ3V0hgF:SbFuFyLVK6g7/+BG+f+Me56SVN2jNq
MD5:	32B590A9694DBAAA28CD70AA34F7029A
SHA1:	81EFAB1546207FFB4B4322C910D8D15817835136
SHA-256:	D31345903C5ABB66505DEBD5713DB002707076B0A82B3DD5EB8AD6B8E6511293
SHA-512:	448BABB293E03FFFD8AA9C1AE71AA72CFB8681D627F49FFDF6CFF4BAED00BE91F631A813D7C2BD696A55B052489B5FDA9F2EB56E353284D52BF1CE9826563F 3E
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=3508d41a6a524398a77538e312fb9162.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:75371M5uFC2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.420374781044546
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+Md6QR86RHQ0jNq:qgFqdg7/+0+f+M4oq
MD5:	FC88EDBD65AD1E0D92C8510B3CCB7DC7
SHA1:	B7609D7338BAB1557456E8870CF339C5B8FA57C2
SHA-256:	4664D924165258B15410B9E6E4FF354BED5064D44917DA1B0375C39BF2AB80F3
SHA-512:	AE098A76984F31A7F510EA9273E23E8DA8984C86DDD6DFF12DC2B32F0A648046A8C56C580657450EF8FA117F5E9E6AC3C835F7DD6688146315B2055435B9A3CE
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=9139b4c70a35413a91bc6a4ee7bbf6e8.IDENTIFIER=gdm-session-worker.

/run/systemd/journal/streams/.#9:75434knm825	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210

/run/systemd/journal/streams/.#9:75434knm825	
Entropy (8bit):	5.52832325394892
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MJ08LzA+jjFQMzKaBu:qgFqo6g7/+0+f+MtzA+dTmh
MD5:	8625C5E13F73111D4704EAE7010710CD
SHA1:	38DDFB6059570245AFD931F79BF483DA140F587F
SHA-256:	0A89F0313D98A76E783AE61C660C803A27794A646E9443C7790B21936774786C
SHA-512:	E5C3374E12EDF5A32A93EF025B6D1970FE957C99FA46A6131CEFA2AB4BF9E906AA82E4CCE3BDB5AAEA77E407532D2566F1F98AEDC2F791D8333668FC584D81E5
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=a062c5cfbb13408da47787ee551c36bc.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:75435FiXYV5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5187994444251105
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M8+5jGV5jFQMzKaBu:qgFqdg7/+0+f+M8ujGpTmh
MD5:	7A714D9FB8451CA65B22357D5AF27139
SHA1:	663CB21F3F3793F237A5D3778A5D19D6DDA4F3A8
SHA-256:	280456937F01AA07640490B6582CB74B7D14EBD15B40237282F307D9DD3555F5
SHA-512:	0BA823AB4A298E0A21BD09C7F1FA930DCBA6F4FD92A5764CC13F062264A3BC3161F1992CB76E92C466BF6F7C6431E17C923C9C7991A752FCF0E48CFFE5DCC52
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=6875a2ea02e5433f88bc44882c776ef5.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session.

/run/systemd/journal/streams/.#9:75467GHZZk3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	190
Entropy (8bit):	5.347503272023148
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm48Aq6DWET8Bv8jV:SbFuFyLVK6g7/+BG+f+M4Yv8jN3r
MD5:	1DB16F68B5177EE14BCD9CA59B67A387
SHA1:	C766AB7769B9BBB8A9411850EA5DB09BE251EA98
SHA-256:	FD3F411C50C40AB5BE6A558A0BB39954EB7606814B9C18A3BF5A70AFA9E67F3B
SHA-512:	176BDFAF5D09707953EF06E5DFF27BE77D99B20B381F3C868551BB89FC5AEDBA4158790B764B254DA6C7173A134CABCA1692DA03C24A560A01831D486C26DA4
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=256f26e8395546f69500a45ffca748fd.IDENTIFIER=gnome-session.

/run/systemd/journal/streams/.#9:755537yx0J2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.41858871728187
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmr/0BcDuD3js+XW7:SbFuFyLVK6g7/+BG+f+Mz14jFmzXvn
MD5:	00E604B490CC812F110430BCEA2BC2CC
SHA1:	E73F19610AA5E04750411BE97AF33FA9D7F71B06
SHA-256:	E2AE7A52BCB33D1A6BB0459B02B466299D58F204243E1B908CB29AD1EAE85AAB
SHA-512:	4F07D7263A94F21AF3C6A38DDDFFD5FA08F8CD7987E83675F87423DA6DA4F89BB9A7D9258D4718174BC0C6F50A7D97A53E9F99B7820302B8479A62BC0B37A02
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=ac919a4c4fee4fad919e78643ab1f6d5.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:75555inBwv2	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:75555inBwv2	
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.392296812450964
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M8zMjvMqjFmzXvn:qgFqdg7/+0+f+M8w3QXvn
MD5:	81F51732B29DF71765A6863E49405021
SHA1:	EF67CCE5886654A19F319AB64F33DC0D4FF4CE84
SHA-256:	F7D63AFC05E73643F036888963516AED4002FD3A4947E67163B6C6318F08A561
SHA-512:	D56CF02493A66846D92D6EA9ECC2BC5EC30681DC48C07070F022923AF7841A6DB056608DC9BB08184A47C6444333AA98E3E659E45FE9B94EF23FA6B5DE7F3D4
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=67aa999bbf9a4eba9b4ac0b048618361.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:76160XB3lL6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.48947839549794
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MyM1cc9hg2jZcH5CHq:qgFq6g10+f+MPc2zmmq
MD5:	67EF95E6A17F998ED2D840975A15F841
SHA1:	9E877840BF17BCF4AA34BA8C8B4C59ACD0AA4A58
SHA-256:	87E74FA06A74D029C0267ED4C89D9AD6F6CB5E83584B6D9A48C3C8C27801A812
SHA-512:	12373BE1038356B5AC38399E03E1FE36FF66B618E05B83B50409E15AEED597C8FF4D67959B7420E57591ED71386240A2A2649458BE8F3EB83D65AA1C98FAFDD8
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=8298fff58c6544849604f5366e2489b7.IDENTIFIER=systemd-localed.UNIT=systemd-localed.service.

/run/systemd/journal/streams/.#9:762248LBt84	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.288242870256225
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5+UAZhcVDE7sjshQJ:SbFuFyLVIg1BG+f+MyKHjtWL0
MD5:	282B5FB0853486761A20F3E614EF897A
SHA1:	813B63549BD6B1D26683CB6A604F802D74919E00
SHA-256:	69FDCA357001BD8A0AD1909ADAA81998141C169915300955D446A4E2DD4AE6BA
SHA-512:	FE5873638707E03A63BA161CAA2A8CD42281B19BB5E9DF8EED319656D469779736314702F00D26B0C67F90BDD91E4015BBDA64DDB30EF1285D8992EAB727844
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=3cec711eea0f4e55a0ce929194ca9a42.IDENTIFIER=pulseaudio.

/run/systemd/journal/streams/.#9:76230E1wIP4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.370641653173075
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MPddRNllmjNALQru+u:qgFq6g10+f+MPdTjl8Wr
MD5:	49C07E38180BA9761F90DAA6DDD0FF7C
SHA1:	43942B2DB8C0568977957F21E63BDE5AC766A502
SHA-256:	0CA0A300E2FA4584F25D0F7120EDBC271F050ECD719DDA29B8C6353FC1F21AC4
SHA-512:	2548ABA5A4ECA515982C893395A66AEEF164D50909287D32D63A9411C1785F85EB05D94792A1E114291093E491D292D439A84C76042E05C509F7257D2844E06F
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=cfdef4566ad14c87ac7c446e3d57dc50.IDENTIFIER=geoclue.UNIT=geoclue.service.

/run/systemd/journal/streams/.#9:763065XzBv6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.411641309795204
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MuHq6DjFmShmWc0vn:qgFqo6g7/+0+f+MOqe9kWc0vn
MD5:	85973D9E278D99820AAEF56D24B23B6F
SHA1:	C05490975089A9382AC663524B5F7C42C36FFEED
SHA-256:	9606925F5808CD5953A6D21325E9BE90332AD05BFC9537916BA04DFCD6D86D91
SHA-512:	9DF45F4A167ADED928C9B420194CE3F1771777A1E1259934B674998DAAD741645698A5317BC10D6F2A5CADFB1665EEC4EA0E5DBF67ACB5443B32FC7EEE1322 C
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=d884348a2637442a88b0db2a9efbd957.IDENTIFIER=org.gnome.SettingsDaemon.Sharing.desktop.

/run/systemd/journal/streams/.#9:76308BpVHP3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.396567834925159
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+Mp73SJEBjFmShmWc0vn:qgFqdg7/+0+f+Mp7SJEH9kWc0vn
MD5:	0E7C4A175ABB4B31C02BCA8C655E0835
SHA1:	C21FDFE4A20F93D0A91BA6382B18DF56E03A1831
SHA-256:	1025292E1BBBBB24D2E05D6CD34421259115D072A668EC599FFFA33D6DFE3FD5
SHA-512:	AF9FB3F582695966F505BC72487C12E4B65D6C1BC57FB560440DFBD6A50CB55CC2AA47DBF216D2BF4F40A5CD292847543710A7F984500184566A852658AFE00A
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=3ddbaf5414b3445bb3e60dd8c35141e2.IDENTIFIER=org.gnome.SettingsDaemon.Sharing.desktop.

/run/systemd/journal/streams/.#9:76330g4YJf4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.442422889623728
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MXHwI2jFmShmVxfvn:qgFqo6g7/+0+f+MXwIE9kVxfvn
MD5:	A8597C646A4A71031278730C265B2B9F
SHA1:	23A55C210DC74C1FBA0097627DEB253B848F0175
SHA-256:	A94C7BD72E2559790D6C21CDCE2417181848B150AC3CA08DE1B1EB5EAF914BF7
SHA-512:	512FDCBCA265E5C2AB34DACAF16913B19E2889E31E3646A1FCEEB6DE3347049C8170655D3622B7595AE2FAD0D15E772973B7C70F56BEFE2DE81F4CA15E3751 B
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=c9e547c0f1e546698b149253daafd180.IDENTIFIER=org.gnome.SettingsDaemon.Wacom.desktop.

/run/systemd/journal/streams/.#9:76332LoY1W4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.4145159128795415
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MoLSpwjFmShmVxfvn:qgFqdg7/+0+f+MoLSp69kVxfvn
MD5:	685E954D8C31A3789AFCAA1D1A3E8F74
SHA1:	802485AB4FB14C847810FEA2C7E40722BB1544BD
SHA-256:	43DC37BAFF3D784EEC34115CA162383846BDE652B92EAFD44EDC5E23722051C8
SHA-512:	727DFA53CD89272C5DC755E7EB524F6A62FDBD50AFF690B0793DEA246C51904DA2D7E5BCDBBBB3E354C403572C5CA7A3A4E174EA8310976D3B2EEBADA089C ADF
Malicious:	false

/run/systemd/journal/streams/.#9:76332LoY1W4	
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=b74b3663a68d4ba394f4d64f3c092029.IDENTIFIER=org.gnome.SettingsDaemon.Wacom.desktop.

/run/systemd/journal/streams/.#9:76334mkGDO2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.470059998971897
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MrmjEJZcBj5jFmShmDxfvn:qgFqo6g7/+0+f+MrA99kDBvn
MD5:	9F3CB5C881E5AB6F32411F99A724F755
SHA1:	AE208F974F63B084220F4E965095CD2D1E292C81
SHA-256:	1E68BA2CDA0D60A6BF451365FC93B35C7BF8D0AD6D653A68C48B1366E221D3F3
SHA-512:	1430EB608AEF45D937E354DB59407C5129B322A1F2C3D1710F1BD7FE0321480B4840478DD42D53EDE2B3414094A86192F6DAC50869931F2A9966DE7369C41DA6
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=55c39fbc43354d4abcb782279ddc5f85.IDENTIFIER=org.gnome.SettingsDaemon.Color.desktop.

/run/systemd/journal/streams/.#9:76335eosKT3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.353871859477264
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M6mtYDAYTjFmShmDxfvn:qgFqdg7/+0+f+MPt7YN9kDBvn
MD5:	F398274A516A6CEC5E5A0A963643B649
SHA1:	0A75EFFF51AF85972C7F31378DB115A73183AC4B
SHA-256:	EF88CBE0E8B233B96FDE91A6B77CA8A03C1EEB7CACA38050CCCE32ADE78CA6A8
SHA-512:	C9A939D1B8D593878D92797C6A7D47733D0A5BBB0DAEE40162BE99BF222A0723BD2E5CCD1DD0B773CAD84F94F124BBC411FBC7ACE6A005B0F7FD94648EEC314F
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=022682e88b3a4238a5893ddea2008d50.IDENTIFIER=org.gnome.SettingsDaemon.Color.desktop.

/run/systemd/journal/streams/.#9:76357xoZyO3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.389797381017773
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MoIxRhuqjFmShmxBrvn:qgFqo6g7/+0+f+MLxt9kxBvn
MD5:	46037383E02046B0ECF6E3DA22E7571A
SHA1:	207E1109DB83BD16EDF6B3907B13F98A3A76BD29
SHA-256:	33418AE358F31812BF833C5E82DCC6CEDBCEC8B504283352BBD81666DE6EAAF6
SHA-512:	9B40C02481214A65C075DEC4DA265CBC8EB6834259A7B4F174774CD82B7CE660ADBC76036CEF72C713E55AD26EF0C65A5646CF9A0240E909F221C9289523A34
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=74a5ea62aa4044229778441868104705.IDENTIFIER=org.gnome.SettingsDaemon.Keyboard.desktop.

/run/systemd/journal/streams/.#9:76359NuVYs5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.4822639951511665
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M/MR5WRT7jFmShmxBrvn:qgFqdg7/+0+f+MELk9kxBvn
MD5:	85414AEABC9DF0B7FD21F9E17EA8BC51
SHA1:	E2FD81A713FF84E291FBB2D1E886B98B99CD1935
SHA-256:	130876F7B18B69C93A290FF5BD8C89B597081CCF49E1E8D04F7A7F680F41FF1A

/run/systemd/journal/streams/.#9:76359NuVYs5	
SHA-512:	1F2C0310A3936E9D60B64576FDC16E08E25FECF88EDD9C898FCCA7F3CC152D3AD1D4EBDB5D1C395CD6473D4616DF172B046FFA47290A210E2300B66B94BC1 8B
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=1c6a917e7ab54bd39f47f5342d63f8cc.IDENTIFIER=org.gnome.SettingsDaemon.Keyboard.desktop.

/run/systemd/journal/streams/.#9:76381auE5A5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.430347727279041
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MuZclrqjFmShm5PKJ0vn:qgFqo6g7/+0+f+MyQ49kYJ0vn
MD5:	943E3255749E3883ED43DD2863BC248B
SHA1:	A9CEB7B70C1D25B52BE788D367C8B9AF5D68025E
SHA-256:	915B571F618378E8A7AFF29D9527A3B8F7913B98315EF1725FBE52E0B56071C8
SHA-512:	EF7AD218A27817A0C48E7B77CF68CCCB185E475899D54C3F34EEE193756018964B60B7409786DC9BD71ECF63D011D186CD7389D5EC2C085B624416424E0BCA1
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=d8a5936d8d194ff0ba0312d98fd473f7.IDENTIFIER=org.gnome.SettingsDaemon.PrintNotifications.desktop.

/run/systemd/journal/streams/.#9:763830pQvs6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.397480347571483
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MiY32jFmShm5PKJ0vn:qgFqdg7/+0+f+MTU9kYJ0vn
MD5:	4174A4AAD80DC0B563DB2B207D2945F9
SHA1:	6BF5AFA1D6E612F941D3D861428298F5639AA42C
SHA-256:	2B80D447FEEB6A2CDD1641B84666D5F0F17E31081182D0C6CC90B148BF8FEFB2
SHA-512:	33DB788D746B4FA5543C6455958F59C5E1B6D962CD66F317A525B4D3B5D8A5981D3B05867E47EC6F45BDE3777AADD724C9B9A80DC6DD0D28A19C40E3A0422A C
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=189b16b4b02e4b3d83e48fadaf03b1b6.IDENTIFIER=org.gnome.SettingsDaemon.PrintNotifications.desktop.

/run/systemd/journal/streams/.#9:76385VOTxQ4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.4698082938322035
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MobwGQTCjFmShmatvn:qgFqo6g7/+0+f+MobvQc9katvn
MD5:	70FB8B1A8A97776D598A6E36394B564A
SHA1:	1BDB48C69D2640428870C57DA276C7A2ECCCEA6E
SHA-256:	9E64E1943E7049AD04A6F4ACF202E04C46B38EE12862331049EE1CD674FFE5F7
SHA-512:	B1C16CE4352CDBF446DDF8E356D455F7250ED3D148DF7A57B29523D2E17D011C9720BD6BCBA75F23D06F078FED3207CC7D278A91E7DA10FD7E4C20B456B55 A
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=b40b009587254e8cb51a169b9256b134.IDENTIFIER=org.gnome.SettingsDaemon.Rfkill.desktop.

/run/systemd/journal/streams/.#9:76386EziQW3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.4698082938322035
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MJ2VdCGGjFmShmatvn:qgFqdg7/+0+f+MY09katvn

/run/systemd/journal/streams/.#9:76386EziQW3	
MD5:	9B96B52D3739BC3D2E3AC4F4537D2374
SHA1:	8AB64080049F2B5677C72CEA1CCE5696ED517EA6
SHA-256:	6B0BB118B7BB4C848F15F577DFFCED6953104CCD4392C2B8314049F2EB628703
SHA-512:	22E284C64F1C757C05051D7A944F49B075A25DD781273AAEA4794E64188EF422D5897111041BE91BE74ADFFCAE87FE27FE39C86C4D5364A7A057AA8378594D51
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=7523d45091844aa3b6c20bc3e45db77f.IDENTIFIER=org.gnome.SettingsDaemon.Rfkill.desktop.

/run/systemd/journal/streams/.#9:76408aTPvm4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.411281264084006
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MaSGYVBP8jFmShmzxvvn:qgFqo6g7/+0+f+MaZYVh29kztvn
MD5:	62538CC997DC143172FCE149DCE72B6A
SHA1:	B5895054886EA8A0520C345BE1CE5A6645BB310D
SHA-256:	DCDAFD8E0D6106B579D761D8ABBAF40878C409B5EA47C10F9CDCC941FE3F6E32
SHA-512:	3D7C6B2A4759474740D5754F1FD472841D1F0FB3DAE386311C518CFE8C644BC00459B50B01C4FEBB5CAA1151AD0E097C510696713ACF5D62BB6FE30D2A03BB B
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=7877d94d1c4940c8aacf0242be3100cf.IDENTIFIER=org.gnome.SettingsDaemon.Smartcard.desktop.

/run/systemd/journal/streams/.#9:76410fdAvl4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.413710802785556
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M8407+sZjFmShmzxvvn:qgFqdg7/+0+f+M8Ba29kztvn
MD5:	83EF2196B585C20ED37435C0A19C3DCB
SHA1:	BD62D82EC19F05B55B7B8F7A8C4AF0810E5E2B10
SHA-256:	8743A1E2D5DC9A7C95E0171C4696E3D0DE797914C68BE6530C7BD743838B4648
SHA-512:	688E3938D3AB3E3CBABDE49CFCF998C04B40064F22DF7E56BEBC7568095D668349BD1681E56D4B2D9EBF3157A8E084A0E09D97A9C57F42AC2C5A154065F1D5 1
Malicious:	false
Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=69a1a5d3371b41a193fbb4df5ca0221a.IDENTIFIER=org.gnome.SettingsDaemon.Smartcard.desktop.

/run/systemd/journal/streams/.#9:76432ajFyn3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.440059754072214
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M8D24xAVjFmShmZBvn:qgFqo6g7/+0+f+M8HAL9kZBvn
MD5:	61B58A95577DEC99C5F54A35BEB67498
SHA1:	71C24E8C9FA93F7ED6F9EC397036534126796C32
SHA-256:	F526D929F9E4FCBC46C373960D7FC2A7F512818C3C319D4564B0B7ECE563BB21
SHA-512:	B06ED27CFD7D2B1482914C53D3714DC1B78B892442037B2418A6ED55538EAA9CEC39DCD86B51E8E73D87B7CBB74E9D999BC6822B17757EE75CF0CABB6ECCE 85F
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=6f2285116d9c47bb8d130de7b4c42b21.IDENTIFIER=org.gnome.SettingsDaemon.Datetime.desktop.

/run/systemd/journal/streams/.#9:76434aeX244	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	218

/run/systemd/journal/streams/.#9:76434aeX244	
Entropy (8bit):	5.3577153464358265
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MXIFTSjFmShmZBvn:qgFqdg7/+0+f+MY29kZBvn
MD5:	9619C8BB9AAAE83676A11E848F4B93FD
SHA1:	CA36BFB3BCEAD83EF2E1417D5513FF7BF6F01C16
SHA-256:	86AF2FADECEEDC65FD5FE3917290776ADFD8CB02DFB9D48E319C6997C627663F
SHA-512:	0EAAD13BFFD840AA0EE45356C03E4034346BBEAF7BDEDC0916C4D43C0EB42E024114FFE774021C02243C1AECE7F886305F34E5906E2C2A1AF7AF82DAFECD4 15
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=e67697acce7b42d6b4440292347667dc.IDENTIFIER=org.gnome.SettingsDaemon.Datetime.desktop.

/run/systemd/journal/streams/.#9:76456UCfvN6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.463349000974038
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MN2K0QSM0ZjFmShmwtvn:qgFqo6g7/+0+f+MNl0Qmv9kwtvn
MD5:	3454265DD1A8AA8E9426010CD5CC6289
SHA1:	D7DBE4C7521C93889F22C16CECF1DC50A8E28A38
SHA-256:	83B1563D462763B5CCA48C05CFB27CA704546B7470A7FE52564E46759BF2CC87
SHA-512:	C8AA81F62E7339EC087CEEDA1B5313600BACF4D95D5D21723A1129DCF7505E2C49A8A620255CE041640AADF89C55E4C4E72AEA7D6A8841E9360402CB6BB514 5
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=acc7165396c84337b57d66553f4cbbf5.IDENTIFIER=org.gnome.SettingsDaemon.MediaKeys.desktop.

/run/systemd/journal/streams/.#9:76458wvCqi3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.470711486988174
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MA9JXeF2jFmShmwtvn:qgFqdg7/+0+f+MAzyE9kwtvn
MD5:	C58574BC08321705EDAE90EE33123507
SHA1:	52A95F33893C6BCDDA4929692F14F2E06ABBB97B
SHA-256:	2F01E835A649163B814C4C06B3C7DBE25094B5EDC12432D0B512CDC8D2F39CFD
SHA-512:	EABF025749B1275D42E4D42CC88379649C42AD2D8A15AC41C348EB896A86D2E16D2F37A1A35E7E0D1D1847AF6A2229B687552CE3A8F9E478CD9FABB6FB3645 0
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=3c539285f9a6487f9f5192cbae60d829.IDENTIFIER=org.gnome.SettingsDaemon.MediaKeys.desktop.

/run/systemd/journal/streams/.#9:76460RqRkg2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.443737810899174
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M6HdnmWQuzy0jFmShmkiEovn:qgFqo6g7/+0+f+M6HdnmW/9kVEovn
MD5:	3359B170C3C459430847371D710FB2FB
SHA1:	AA6E1C081AE7D74DC6A32A832BBEAA0F0A228F06
SHA-256:	73D5E04538F04311DA4E885F7CFD468C89AA0A7D4E8CEA900CF931DBF91AB639
SHA-512:	C2FFBB84F39CAD1E97541368AA15E7E37289232F5F306B1957AB9E58A37979F024A6839CE8B363326017C6C1DB61E778A8328A8228DA9437738B305C1DB985C6
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=933dcb886dd54387ab0f8deaf354b584.IDENTIFIER=org.gnome.SettingsDaemon.ScreensaverProxy.desktop.

/run/systemd/journal/streams/.#9:76461oocl62	
Process:	/lib/systemd/systemd-journald

/run/systemd/journal/streams/.#9:76461oocl62	
File Type:	ASCII text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.457355383902703
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MuMQYLlRqjFmShmkiEovn:qgFqdg7/+0+f+MoYLb49kVEovn
MD5:	DD0AD72DD4FB815A21FA0A67F06D9F58
SHA1:	8C3CD55772F276EAE03D4449B4B650FD9326091D
SHA-256:	886A50B2A4726111B1EF6A718C0E5F74092086AC9EF6D6AD6627F93AF5926EA1
SHA-512:	D49B2E287D82936FF3E1D2B1FFF9CC78E6F85A8B467CE8A56002FBA34AF33B995A5671DD120F3D09F7E03E033FDAB3C8C4DC050F1B8BD77B62B61D7A81BB3D11
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=db192e8f879a4bd6bdd7d3ffc6f86b9a.IDENTIFIER=org.gnome.SettingsDaemon.ScreensaverProxy.desktop.

/run/systemd/journal/streams/.#9:76483ZGiAv2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.364538850627429
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+Mum9mGxsv0jFmShmpvn:qgFqo6g7/+0+f+MPgAV9kpvn
MD5:	24D4A519851043AEAFC507336D687EE7
SHA1:	1C5BC4B20239F633C6358EE12CBE85EE0902CD4B
SHA-256:	D08268884997DA6D5EB33F9D87452488D5B6A9683356380B0933DA4EA3B033ED
SHA-512:	EA22BCE9414EAD67C7982898D22398115178B4F726CD01891D14FFD3FD227302BEB7098E7A6FD8F68A2590F443FBFFF2A500AED432BCA32CB174550985F5DED
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=d60d206106804ee5b2c4299d9d097dd6.IDENTIFIER=org.gnome.SettingsDaemon.Sound.desktop.

/run/systemd/journal/streams/.#9:76485eABpA6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.475582120306161
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MoqRmNSq0jFmShmpvn:qgFqdg7/+0+f+MVEND+9kpvn
MD5:	7F7579D4A3AA842D781AA9EDA80FC928
SHA1:	BD68ECA2DC89A571FBCC4E1EB17FEB09091D3C67
SHA-256:	E4CE5BBCC3E0256347FF617BB86FAB6A9A8B078F1608EA31BF82292CD62F4024
SHA-512:	6EF17B2A9FA748C3464BADD1E387071B840B55DF7673DB56210918BB8C49FFB602E59A6E631C31B589F86A4910EF716978D538C6461FF029B10AE3D19FC1BBE7
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=af06dddb518c4214938f58819757c923.IDENTIFIER=org.gnome.SettingsDaemon.Sound.desktop.

/run/systemd/journal/streams/.#9:76507TAcBq3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.472118961812767
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MJu9zVljFmShmQmc0vn:qgFqo6g7/+0+f+Ms7b9kQmtvn
MD5:	9270F5091A7F9D25E2529ED311EA5BC2
SHA1:	04EB611B926489289F670E3FE61E27AA7FE50FC5
SHA-256:	226FA66B296092E1A109F9154345C37BCEFB3ECF047352143380D32CCD7C2E25
SHA-512:	E1B32CD5292B6B69521FBFECD15E8BFE784A156B3E0CC6EBBE527CB8BFAB69F699AA1B537E2EB44229580DE6B9FE28883F5D49CE74AE7DAA1B2829EECD0B5503
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=1758df3fcbbb42eb97866a908f9fcd12.IDENTIFIER=org.gnome.SettingsDaemon.A11ySettings.desktop.

/run/systemd/journal/streams/.#9:76510yF3hG6	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.460275761438485
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MSRsBMpF2jFmShmQmc0vn:qgFqdg7/+0+f+MjBQE9kQmtvn
MD5:	5032CF68C6EF949637BCEC354A2522EC
SHA1:	B0DAFDD08FED723B36DB8039F08E30B4358A6573
SHA-256:	58132CF0EB3B31FF913E02634985F70B4308020D3439C8238ACCF2A4653B80EF
SHA-512:	9C452D312F0139DA810AC292DBF44AC921BAAFF85C66C3A9925789D2134DFE10D588C684461829BBD4D6062342F0A210642730AFA148584A2FE7C16679D1007B
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=3ff7ee0d69324fd19562c3c46bf73bb4.IDENTIFIER=org.gnome.SettingsDaemon.A11ySettings.desktop.

/run/systemd/journal/streams/.#9:76531EWnHJ4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.442141385091807
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MoWMhf4kjFmShmx+0vn:qgFqo6g7/+0+f+MoV9k40vn
MD5:	89E4199A19B3172809F3BA833C5D53E1
SHA1:	B3B50E86AFBB179357DEA7E16AEC9B591661CE6D
SHA-256:	CCC36E07DFE0B3C6E09C2F33057A7DAA4114FF2D5D4B1E86723FDA80FFB13FE1
SHA-512:	70F2473A74D8FE5A44577B938AF9F172C422E053E728AB0898387DD63B13C8929D6207F78FCD8CBB86305DB4CCF63BD322555BBB44FB669409E8A008C9772E48
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=b9aba3f570ce4eba9156e72cbc67dc42.IDENTIFIER=org.gnome.SettingsDaemon.Housekeeping.desktop.

/run/systemd/journal/streams/.#9:76534i5VJV3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.449149910629764
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MWIkAjFmShmx+0vn:qgFqdg7/+0+f+MWIkK9k40vn
MD5:	F1992EB84D7240BB9E62F747F668EA30
SHA1:	86AEAA736281FC7BC41B8CA510C6DF5D170B903B
SHA-256:	4003D52893632D5DC22CDC59D4E516014A8EA2659C0627240FE3E07B029219E9
SHA-512:	C2325FDA5E6A37249933877DE1F901F24DCC54436DE53E39E3DD347998E7109F81EB560065B6BC62D2B923B384A12094802A0B1A006ADDFB1AFC4039E9E174C
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=396f56152e304f298779a02638f5fe32.IDENTIFIER=org.gnome.SettingsDaemon.Housekeeping.desktop.

/run/systemd/journal/streams/.#9:76557ws54k2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.41314231880886
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+MbnwjRqjFmShm3vn:qgFqo6g7/+0+f+Mbwj29k3vn
MD5:	0F2068026D627C20AED842ED4BF6FEB6
SHA1:	14982081A314C744CB17D7315E6681B0D896131E
SHA-256:	42253AB3AAEB33E4DE224CE31B49B0FABD71BAFFA2859EB843AD4448474A44FE
SHA-512:	F8C5B711B9D6119D76F3CD7D7857201FCE4E7550902334DD8248D512B9FD848B4B60ECAF378D01A56070AFBE48ACA1FA44308F4DCEE595C7F4CBE1987DD7FD4
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=11b8eb6eb81c49f6bf492a8e45e4942a.IDENTIFIER=org.gnome.SettingsDaemon.Power.desktop.

/run/systemd/journal/streams/.#9:76560x28BZ5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.4084747021686255
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmrmSWHSTNBqjs+XE:SbFuFyLVI6g7/+BG+f+M5UzjFmShm3vn
MD5:	0F8708A224F5B7CB2D9576FF743CF218
SHA1:	E59A766380C23EE710BD4D86723C51C0302DDBA5
SHA-256:	395AB885B8A907D88EEF1D4A56D5D603E2A47C93D4F4440FC837E52B85E6D479
SHA-512:	B7727FB5C07FAF042AE4C5FEF875592E82F27A61E33DFC3A7D57E3478E756DB595EFB64E06A05EB1DC675285FBA12E26012340C35B1CA88AE46FC76CECE18A C
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=ae8a35a73dbf4672bac7e2eb97d4e46f.IDENTIFIER=org.gnome.SettingsDaemon.Power.desktop.

/run/systemd/journal/streams/.#9:76748i9hEp5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.446604102038905
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+MrRsuUJ0jZcHdzqDq:qgFq6g10+f+MFsomQDq
MD5:	A5AB2760278D7D8B807D54CAC042C225
SHA1:	F7F7D185CE06C965AEC0E8F827F85D4922A53777
SHA-256:	4ACC3CA7B50969EFDD04B1D3DB52B14ADFD50DD14DABE14CB4CED050086E8C47
SHA-512:	1F4E62ACFE4DB93BB48DFF7B1898BC8CD709479BC2AFA0A7DFDF146856296E2E4FBBCE6E955408A832602170A4B7294E10DED093CE5CDF21D9B29D4A6A4A6 DE
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=e7f5cc649e74473a9fc816ffb3573a10.IDENTIFIER=systemd-hostnamed.UNIT=systemd-hostnamed.service.

/run/systemd/journal/streams/.#9:76853YjB3v5	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	190
Entropy (8bit):	5.4015278115309915
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmrQlGkBBSAVW/0T8:SbFuFyLVK6g7/+BG+f+M8BBSd88jN3r
MD5:	0C4063AA79842EA0970F7AEE33B6E427
SHA1:	C466D4FE103D0DBBB3F1D0A2E324EA22BA236F57
SHA-256:	941A7E609C3D0687C6C988F7CF39A02B37CA1A3C8714EB27B9E50AC9C2E77A29
SHA-512:	AA7615DC067DD1519452D493DEC47362935D13FAC24A67083B612A5A4C8EC08E10C6B527C7D576CBD24F56FA2F0C77D73D9D1E307DEB9309C6AAC276C09D0 A
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=a69fe1cd7d3547f982313b43d93d596f.IDENTIFIER=gnome-session.

/run/systemd/journal/streams/.#9:769693YyTV2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.4441194523339655
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+M+ARbaTjFmzXvn:qgFqo6g7/+0+f+MJkQXvn
MD5:	919E996E0F3B169FFF88E5F8AF084CEF
SHA1:	28399A129DE96C9284069C271140BC802B55293A
SHA-256:	E8C0B54DCB4661882EC8800EC73EE0224755BD5DE4458168E40AD5BB82FC78E3
SHA-512:	EEF5BAB0AD40F593A87CA8BCAC7DEAB147125EF2D1E5C66B0ED12228690D724E9639029DA743DFA7BF7A7E0D153BA18F088A26F03FADC5A4DBEFB5EEC4710 8BB
Malicious:	false

/run/systemd/journal/streams/.#9:769693YyTV2	
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=e8126ef75d3748e4ac9bae49326bd8d6.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:76970d4BhP4	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.434734217616036
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+MeoIFeAjFmzXvn:qgFqdg7/+0+f+MeouQXvn
MD5:	7D811C939BAEBBADA0F0D8AD48CE6B71
SHA1:	F98767CC41E6A127871DFA05D7CBADD745CB9FB1
SHA-256:	AE7E1DBD4D0A5D873FAA1FFE25A338C752140EC06F17DC3EEE30A52220658890
SHA-512:	7E230A8ED489E28167122B618C1348C1280FC824EBCF43E01E4A1A84ACD4EED9130077E384E360E705B826291D00E2688DB7DD300D9BF948DBFFF407AF8E73B
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=7ba42b1495344a16b19ee7913769f265.IDENTIFIER=org.gnome.Shell.desktop.

/run/systemd/journal/streams/.#9:78098P3rsq2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.459832518865926
Encrypted:	false
SSDEEP:	6:SbFuFyLVIg1BG+f+M45lEpTkeF2jdCt/rRMtq:qgFq6g10+f+M45kTTcCDL
MD5:	A3D089664A7E51275F148CF18BA92EE6
SHA1:	62926BC86EFB17A59F263EC4DECE8A0C7218273F
SHA-256:	BB46F1FC2B5E60AF33779A698EF8855489EA67778A12A9B113A44A598673D757
SHA-512:	37359AE749530252045061A8C38758083908A45E2D77FEC3957611AB0A6843D2A9403B3F3550AE960F1784E7BBCCF0253916F482E4373F0470861A249320D715
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=2e7a218e58384fd9bae37368c198b26e.IDENTIFIER=whoopsie-upload-all.UNIT=apport-autoreport.service.

/run/systemd/journal/streams/.#9:78341pQFg34	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.431099278942942
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmukdAOt6klMqjsicWC:SbFuFyLVIg1BG+f+Mukd9fjZcH5CHq
MD5:	9BBC96E7EAC499AF94676042FD18CE1F
SHA1:	0AF6AF1C437658418A014A72B9BB2A80A55A6AFA
SHA-256:	EFB1E5CE9DD38B78E24EC29797A7DED2786329CDC0BF0B076695405693706D60
SHA-512:	DBF3E0BCEDA24FE679447DC25AB615324DB410FE76D0B9D78F50CAF5379CE0B05265D85014813B27AF9F80F1F692348D4581ACE455A5999BB80096F283BA7BF
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=dba82565e84a4d0bb4556af3aba1d994.IDENTIFIER=systemd-localed.UNIT=systemd-localed.service.

/run/systemd/journal/streams/.#9:78493qF5285	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.325763267645582
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmsydpSm0GPGA90js3h:SbFuFyLVIg1BG+f+Msyd2GPX90jXjK
MD5:	C83F4FC50D6CF09AB67C8E076CC4DE2C
SHA1:	8223C5412AFE1162F362ACC18ED9865DBE29CC49
SHA-256:	1311794C1C88B45894C0BACD15E4654FD416E394EBA9C590559EF26167CC6FBE

/run/systemd/journal/streams/.#9:78493qF5285	
SHA-512:	A0F065C04A8C604FBF9BD4FFA12876F24EF9EBBD339577ED5F5ADF2FE3215149F9A0875548316621B4B8A40219A1CDAE2CF846754FBB4D12E685CDFC96E08C7 5
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_
	ID=f43bfdd970dc4e8bb3ca500faece1f7f.IDENTIFIER=fprintd.UNIT=fprintd.service.

/run/systemd/journal/streams/.#9:78547ifZ413	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.398555117995437
Encrypted:	false
SSDEEP:	6:SbFuFyLVK6g7/+BG+f+Mu0cmJsjZarvn:qgFqo6g7/+0+f+M9cmJ6arvn
MD5:	E72F62BA3365857195709C69F1305815
SHA1:	0B34429379717553 70AC6242781CEBF253FB2A53
SHA-256:	A064EA33C632EEA2D177C2A6AE0E1D35F083FB0BE1F1A1BAA377AE23B84B7FAB
SHA-512:	95AF8CDDE6371C51FD5A9C06D870946DF40ED5588E7508FFDF8FE84FAAB5B64B15CCD19FBD0E0EBECD588E341E612D5608111AF29F31F72BE61B947E6C75D/ 0E
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=5e65cbe9d51f4f7083e60ea879ca9cf2.IDENTIFIER=spice-vdagent.desktop.

/run/systemd/journal/streams/.#9:78549lp0QP3	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.391257928914345
Encrypted:	false
SSDEEP:	6:SbFuFyLVI6g7/+BG+f+M+oqTA22jZarvn:qgFqdg7/+0+f+MuTuarvn
MD5:	2E8A4D7750DE6DF180E08149A91E33D5
SHA1:	55F54838C2C6EE0047870447DD6D3BAB4D336E29
SHA-256:	432467FDE29E8FD7FE5EBF6C898CBA9F21671A17DED13CAD8A35D04BD2C34B5F
SHA-512:	0BA5CD425FD618AB7F708D23E3D6A66C4FA79C5AEBEC3BF8556ECC5672D62A8D7371D595927E83C9A7201E3A99F1349284C6346E93793B112D737C917215804
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=53b6cf34cfdd4b608a98c5c9280b4d03.IDENTIFIER=spice-vdagent.desktop.

/run/systemd/journal/streams/.#9:785806rkdQ2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	192
Entropy (8bit):	5.334196467240052
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmu8cTzAHwumTATjq:SbFuFyLVK6g7/+BG+f+MuLumkTj022vn
MD5:	54657099FD9B54DB7A7F1EEFADDFAB6F
SHA1:	4294E44E237E4F6DA2059F3A8500834FA5FFF296
SHA-256:	C1DD3F9E7C27688513EEF8304E195F361858B41A5B98BC5782F814576F7B64C5
SHA-512:	FCD96C3035B9F5FABA5AA0CE0466585010BB08A42F943638EF756B86A8FCD4ECD8F0AE82B80CAD73D16832EC0FE5EAEB24C386FCC12B3A4ED740C9511A574 B8
Malicious:	false

Preview:	# This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I
	D=dece5975cb1e4d15bebe078e95a49b8d.IDENTIFIER=xbrlapi.desktop.

/run/systemd/journal/streams/.#9:78581rM4oc2	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	192
Entropy (8bit):	5.366690378477175
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmp6ITcSMVFGXzFlL:SbFuFyLVI6g7/+BG+f+M1Mu2j022vn

/run/systemd/journal/streams/.#9:78581rM4oc2	
MD5:	F267268694FBA34E43AD18A1B131ECED
SHA1:	1BB31D015B9B5EA973B437BB7A084FD09BB817EA
SHA-256:	CC0FE381A20BB059A9CEEFC47B59473B0F79FD171AF298E642E345631375CD34
SHA-512:	E374AE31F8C21D4EDFE9452CE945DD618A417D73C858B04D1DC2DC33E44EE2A7CF7B16D4A0625F98F72D837FF8C688D56B631FC329B269707C776548E98B1D
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=cd965cd2c00646e797b0c0574fc2b3bc.IDENTIFIER=xbrlapi.desktop.

/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:DSt:8
MD5:	B7A1FF7A2872E02F2C4A3A950A658E6F
SHA1:	0E3105C99B10616AF96E0F50F7714C00897BBEFA
SHA-256:	8BCCB7E04C810A6D9AABBC81B5662FC52FC1BD1EC089807E560FA4FA0E3B50E4
SHA-512:	A8F572B14F32BDEB1AF4A3A5E17348B9D5DC3B5285817FDFC983B0583A0175480210C43D2A19D060805353A645C1205D89B9583F57CC5D738D98E8DE9D59B5E
Malicious:	false
Preview:	5378.

/run/user/127/ICEauthority	
Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	6.028621580012958
Encrypted:	false
SSDEEP:	12:OxPBep+9ZOveY+BeRNrxPSBCoEiveY+SjxP5mhijveY+5tWmxPwWoveY+wcZVveI:A9ZbCoEUwqra1XOu
MD5:	140602876E8D29AA3BC885BB131AE266
SHA1:	2A7B0D8A8C3DEB38D72A14894CF741BF9B2C15D4
SHA-256:	DAD4D076EC3FC63284B4DF943BD4EA12B2C92C91F059E65805E2CCD6C3A52508
SHA-512:	D6FD23AC4FE2D741207E2603A54BD98ACB0CD60D8E78A5A1F675787CA1BD4558CAF3A9CA023BFEED9C4AC6DF0E47C3D8EC4DBDB20C60DBABE2A182F4B3CB9A01
Malicious:	false
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5515..MIT-MAGIC-COOKIE-1....N.W..;v.}o....XSMP...#local/galassia:@/tmp/.ICE-unix/5515..MIT-MAGIC-COOKIE-1.....fD.z.j^..W ^..ICE...!unix/galassia:/tmp/.ICE-unix/5427..MIT-MAGIC-COOKIE-1....R. .o.....~..ICE...#local/galassia:@/tmp/.ICE-unix/5427..MIT-MAGIC-COOKIE-1..%r.au..:...m. ..XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.....A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....o.(R...}.9.. .ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f.....E..c. .XSMP...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... .....Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,.:B.o.. ....ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte\|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN.....N+ ..$..XSMP...#local/galass

/run/user/127/dconf/user	
Process:	/usr/libexec/gsd-power
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	93B885ADFE0DA089CDF634904FD59F71
SHA1:	5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F
SHA-256:	6E340B9CFFB37A989CA544E6BB780A2C78901D3FB33738768511A30617AFA01D
SHA-512:	B8244D028981D693AF7B456AF8EFA4CAD63D282E19FF14942C246E50D9351D22704A802A71C3580B6370DE4CEB293C324A8423342557D4E5C38438F0E36910EE
Malicious:	false
Preview:	.

/run/user/127/gdm/Xauthority	
Process:	/usr/lib/gdm3/gdm-x-session
File Type:	X11 Xauthority data
Category:	dropped

/run/user/127/gdm/Xauthority	
Size (bytes):	104
Entropy (8bit):	4.942288416944157
Encrypted:	false
SSDEEP:	3:rg/WFllasO93r7hAcJtWFllasO93r7hAcv:rg/WFl277h5LWFl277h5v
MD5:	7227465F20352542388694FFCB3DE618
SHA1:	ABA5AD0644AC0133DDE401FE35BD9CE0B7E76949
SHA-256:	ADF27BBFEF607013F8D33B56BFB926DC188F2D6E8BD098B823B8E09A6471F1BC
SHA-512:	49BF9887B49518F7F97370ECB8B767BCDBDB174211B11B87FEA0D6506ED3CE9485C9699FBE67F7FBF4CF394B91E4D6D77920BECA81EF440902DB6B7FF4B2C4 2
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1.....x.M.....9[.....galassia....MIT-MAGIC-COOKIE-1.....x.M.....9[.

/run/user/127/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:HT2n:z2
MD5:	A153D32C59252FD4D55E3D757A7BBF39
SHA1:	6C3807886D9A36F46925E3739E323A3CBB8B619C
SHA-256:	01A7F5CE7902631B3E6F48EDD80A338B48168FE561EA2CB6FC41846D419C0E00
SHA-512:	1B476406824C34E30484340DD35B60A4C041F417E6D753727A1DE53B74B6CDAD5D95A37601C8845551519B3B40CA32E8C34D4B63B338F6EC98369F78658B1121
Malicious:	false
Preview:	5761.

/tmp/server-0.xkm	
Process:	/usr/bin/xkbcomp
File Type:	Compiled XKB Keymap: lsb, version 15
Category:	dropped
Size (bytes):	12060
Entropy (8bit):	4.8492493153178975
Encrypted:	false
SSDEEP:	192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ
MD5:	B4E3EB0B8B6B0FC1F46740C573E18D86
SHA1:	7D35426357695EBA77850757E8939A62DCEFF2D1
SHA-256:	7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91
SHA-512:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE0 1
Malicious:	false
Preview:	.mkx.....D.....h.....<.....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta ....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD 06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB 08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP 3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWN PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181 I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18

/var/jbx/logs/jbxinit.linux.out.log	
Process:	/usr/bin/umount
File Type:	ASCII text
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.456174630069642
Encrypted:	false
SSDEEP:	3:dGT+HlNTcbUhHyI:mMlObUcI
MD5:	DD6E25C1ECDB6D7867C56B78EE738DFB
SHA1:	4C945281D8B7527AF05CC96B98F1DF62768805E2
SHA-256:	5FC419CFE7B06D07BCED5CD01F5D648C852171EA46AA3F7DA28D6EBF8C571E6D
SHA-512:	FFB8BE08FE6FD1958904B02D61FAD978FFD147439E028F29CE872C959EFDB2F060F7F34E75C1DA7C54779D934FF3A9B602391DEDCD1233FFE960BF47A5A4361
Malicious:	false
Preview:	umount: /var/jbxall (//192.168.2.1/all) unmounted.

/var/jbxinit.linux.py	
Process:	/usr/bin/srm
File Type:	data
Category:	dropped
Size (bytes):	1245222
Entropy (8bit):	6.017979416652393
Encrypted:	false
SSDEEP:	6144:YiH1wLU2rjYuAt0WiN4GjfvVRz/FPFjbNBiWdKFv3d9PJdMr0cxee95:Y8+rjvWIxLvVRz9RBBi+KFvvJdg75
MD5:	20A785E7D61F0CE67DF6C985A2F1634A
SHA1:	B60E5CB9ECF2913EE61FC6CA7E0723992E2A5C31
SHA-256:	3C7EFEA23C0F34C2803E18B3EFDC1783542F886AD750E5DA5FDDA71C7085539F
SHA-512:	9D3B91590C86B797DB43C9956F0A7A0275DA02CA345A143074C849BE0A3A8011DF10183829AEC859C100106B472EEAAF425147BF223EBEC3F6A18CA454EA4DAD
Malicious:	false
Preview:	....

/var/jbxkick	
Process:	/usr/bin/srm
File Type:	data
Category:	dropped
Size (bytes):	1245222
Entropy (8bit):	6.017714475480917
Encrypted:	false
SSDEEP:	6144:7kpiQuv6JhmBCXgReBFKCP0ualxDGfBx7kRSxhk6gJ/q8oUGVVNdG7thaZAb:7kpiOJhCLRM0BDGZx7k6k6I6dGmZ8
MD5:	4E0771127BE63FB9C141EAB7454F981B
SHA1:	FFC612C9CC40913A76B33ECDC9943F9898E8BB25
SHA-256:	814DF5D9E40FD8B8CAEE172777C58221E54F4F7126380E3434973821159416DA
SHA-512:	B8D28AF2BA485D31E1153B7DE0538DCD2A2B333D4C74E75FFEB681BB1E67889A2D6FA3B42F7069C309E49178FE49DE36167C80619794EB9E76500C5467C1E6B
Malicious:	false
Preview:	....

/var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0	
Process:	/usr/bin/ibus-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.109102016666785
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWpB7hX19D:q5sU3LWfLUDmQymqSFbfomSt7hXfD
MD5:	11ACA7193B40F94BF32F26306F66550E
SHA1:	5747BC1B3CF2E06AF256A5C9783788292AEF2028
SHA-256:	6A78D34F6E91F7E2F306718D8A42350B5469251A4F0B8E3F9039283BE0A37109
SHA-512:	7CFF4DF86D4A748D019F1B58B34A0EDB831BB5EA3336402743CAE4B38633A9A9139FC9E3461A24B1D87904CBE0FA8AA63ED0A4BB2832B242064498AE3FD8EC57
Malicious:	false
Preview:	# This file is created by ibus-daemon, please do not modify it..# This file allows processes on the machine to find the.# ibus session bus with the below address..# If the IBUS_ADDRESS environment variable is set, it will.# be used rather than this file..IBUS_ADDRESS=unix:abstract=/var/lib/gdm3/.cache/ibus/dbus-84UEtShU,guid=f9c52ac62c2ee3a279f5ac3c61807a1a.IBUS_DAEMON_PID=5623.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE(9
Malicious:	false
Preview:	.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE(9
Malicious:	false
Preview:	.

/var/log/Xorg.0.log	
Process:	/usr/lib/xorg/Xorg
File Type:	ASCII text
Category:	dropped
Size (bytes):	41347
Entropy (8bit):	5.277717882033828
Encrypted:	false
SSDEEP:	384:qtG8/XbzlMqZdUd/dFd+dzd9dZdcdmdKdedHd+dOdbdKd2dwdVdQdWrdSudVtdEt:4G8PbyqHgVP8V6pJpQG4
MD5:	8D756A104E1A50A90AC6F3183AD13E22
SHA1:	3C32A6071A51BD2129772010B4519802A67D3E85
SHA-256:	629F440F3E03DCC2FE16CF6313D7A90127AA765E89A97CFA3B2432B0E6DF876D
SHA-512:	D64F3DBC8DEAEBDF198D634361AE85B300C966A30198658A1EEB5152B67102767B8A8775A4667156A057BF669AA8A837AFCC182AFAD4385B2779A30F4548D78I
Malicious:	false
Preview:	[501.445] (--) Log file renamed from "/var/log/Xorg.pid-5494.log" to "/var/log/Xorg.0.log".[501.469] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[5 01.482] Build Operating System: linux Ubuntu.[501.491] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[501.500] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[501.5 14] Build Date: 06 July 2021 10:17:51AM.[501.519] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[501.527] Current version of pixman: 0.38.4.[501.536] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[501.546] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??)

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/system.journal	
Process:	/lib/systemd/systemd-journald
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	1.4084232590067822
Encrypted:	false
SSDEEP:	3:F31HlxNebZNe5:F3
MD5:	E11866F0B4B24883E359C306B6B4DA09
SHA1:	ED6595EF0FF664C1825100508698650DC6A8B840
SHA-256:	39FA6E4A6AD76CCAA0C7B20434E35C402DDFF76D51F2CD037BDAD5F36491B6A2
SHA-512:	8A85F9308B678771F2A79E1891DECFFBEE1A3AE5756392069C5E8A1CA95EC71EF2577CED0E95365E04020565D5912DCA614BBD86525E57A1E8243F7DB683006I
Malicious:	false
Preview:	LPKSHHRH.....O...R.;.YD.....O...R.;.YD.....

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/user-1000.journal	
Process:	/lib/systemd/systemd-journald
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	1.448047321524811
Encrypted:	false
SSDEEP:	3:F31Hl6aVdwX/SaVdwll:F3BPAPg

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/user-1000.journal	
MD5:	98FAAACC4C0AFFE9DA3DE5FE20A90BF4
SHA1:	DF5C6A77BA4A3D4994ABAF97934D55B310B24627
SHA-256:	6551F25B6C2D53691A4B28392C244EE4ECE81AB8051025D53734BA9654507C9D
SHA-512:	DBBC79C0520C3C335183E76C78F6D65013F7AA0DC6BA340583B0BA1B8F949542FB66374A7EF1E29CD5530264FE1CDC410EAA3C49B5D0C90FCA57F3F6E62311B
Malicious:	false
Preview:	LPKSHHRH.....y.S?.B...Zu+.@).....y.S?.B...Zu+.@)..... .....

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.524983795123989
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	SZAYTvvY9Y
File size:	100836
MD5:	f274fb7e2b929c40da1fcc2c0ed1db8b
SHA1:	a0285f5e70c6dc90815d065f527b26b7e54cad06
SHA256:	6708e5ebbe503d06a63775601a9bd50a592d7e8bcbe142975635a51128bfb895
SHA512:	c1f4277313965bbc2b7fa4c928979a8656e3a3beb2fc8ab0fdec4c90806d2e399c6488ef14d5c6ef18000850b323a2f49df6ca657af6c9ba58b7ad054a64fc13
SSDEEP:	1536:om9+W1PX4QgNm/j1CuFSQpFufc93/nOL01hLqM/:79+W1PX4Qgw9f3/nk0Gc
File Content Preview:	.ELF.....`.@.4.....4. ...(.....@...@..|...|. .....E...E.P....+.....Q.td.....<|.. '!.....'.....<X..'!... .....9'.. .....<(..'! c9

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	100276
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x16300	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x416420	0x16420	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x416480	0x16480	0x1850	0x0	0x2	A	0	0	16

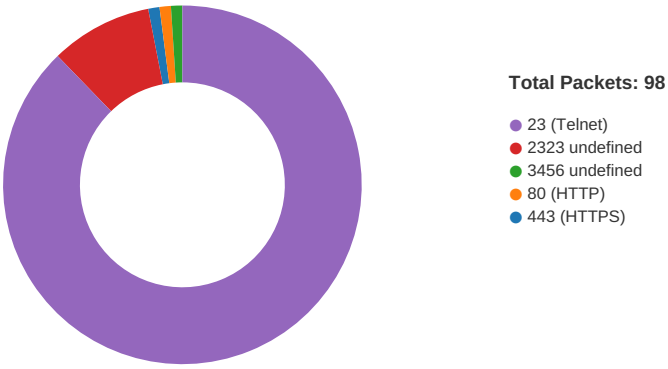
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.ctors	PROGBITS	0x458000	0x18000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x458008	0x18008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x458014	0x18014	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x458020	0x18020	0x300	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x458320	0x18320	0x430	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x458750	0x18750	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x458780	0x18750	0x2388	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x8ca	0x18750	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x18750	0x64	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x17cd0	0x17cd0	3.5842	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x18000	0x458000	0x458000	0x750	0x2b08	2.3386	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: SZAYTvvY9Y PID: 5243 Parent PID: 5112

General

Start time:	23:34:49
Start date:	01/11/2021
Path:	/tmp/SZAYTvvY9Y
Arguments:	/tmp/SZAYTvvY9Y
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Deleted

File Read

Analysis Process: SZAYTvvY9Y PID: 5247 Parent PID: 5243

General

Start time:	23:34:51
Start date:	01/11/2021
Path:	/tmp/SZAYTvvY9Y
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: SZAYTvvY9Y PID: 5248 Parent PID: 5243

General

Start time:	23:34:51
Start date:	01/11/2021
Path:	/tmp/SZAYTvvY9Y
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SZAYTvvY9Y PID: 5250 Parent PID: 5243

General

Start time:	23:34:51
Start date:	01/11/2021
Path:	/tmp/SZAYTvvY9Y
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: systemd PID: 5255 Parent PID: 1

General

Start time:	23:34:53
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5255 Parent PID: 1

General

Start time:	23:34:53
Start date:	01/11/2021
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: 5275 Parent PID: 1

General

Start time:	23:34:53
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5275 Parent PID: 1

General

Start time:	23:34:53
Start date:	01/11/2021
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: 5280 Parent PID: 1

General

Start time:	23:34:57
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5280 Parent PID: 1

General

Start time:	23:34:57
Start date:	01/11/2021
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: gdm3 PID: 5324 Parent PID: 1320

General

Start time:	23:35:43
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5324 Parent PID: 1320

General

Start time:	23:35:43
Start date:	01/11/2021
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: 5342 Parent PID: 1320

General

Start time:	23:35:43

Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5342 Parent PID: 1320

General

Start time:	23:35:43
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: dash PID: 5343 Parent PID: 5113

General

Start time:	23:35:45
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xdotool PID: 5343 Parent PID: 5113

General

Start time:	23:35:45
Start date:	01/11/2021
Path:	/usr/bin/xdotool
Arguments:	xdotool windowminimize
File size:	81192 bytes
MD5 hash:	38ea1b4bfcc631da4576723b24e1510e

File Activities

File Read

File Written

Analysis Process: python2.7 PID: 5344 Parent PID: 4485

General

Start time:	23:35:45

Start date:	01/11/2021
Path:	/usr/bin/python2.7
Arguments:	n/a
File size:	3674216 bytes
MD5 hash:	5b48b7b247d786dc3f7be8e53992ea63

Analysis Process: srm PID: 5344 Parent PID: 4485

General

Start time:	23:35:46
Start date:	01/11/2021
Path:	/usr/bin/srm
Arguments:	srm -fr /var/jbxkick /var/jbxinit.linux.py /home/saturnino/.config/autostart/jbxkick.desktop
File size:	22656 bytes
MD5 hash:	5d0db044b173f989a73a0790b19e79fa

File Activities

File Deleted

File Read

File Written

File Moved

Analysis Process: python2.7 PID: 5347 Parent PID: 4485

General

Start time:	23:35:48
Start date:	01/11/2021
Path:	/usr/bin/python2.7
Arguments:	n/a
File size:	3674216 bytes
MD5 hash:	5b48b7b247d786dc3f7be8e53992ea63

Analysis Process: rm PID: 5347 Parent PID: 4485

General

Start time:	23:35:48
Start date:	01/11/2021
Path:	/usr/bin/rm
Arguments:	rm -fr /var/jbxkick /var/jbxinit.linux.py /home/saturnino/.config/autostart/jbxkick.desktop
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: python2.7 PID: 5348 Parent PID: 2258

General

Start time:	23:35:48
Start date:	01/11/2021
Path:	/usr/bin/python2.7
Arguments:	n/a
File size:	3674216 bytes
MD5 hash:	5b48b7b247d786dc3f7be8e53992ea63

Analysis Process: umount PID: 5348 Parent PID: 2258

General

Start time:	23:35:48
Start date:	01/11/2021
Path:	/usr/bin/umount
Arguments:	umount -v /var/jbxall
File size:	39144 bytes
MD5 hash:	2a1758ef6cf863f285bc8a918edbc0be

File Activities

File Deleted

File Read

File Written

File Moved

Owner / Group Modified

Permission Modified

Analysis Process: udisksd PID: 5371 Parent PID: 799

General

Start time:	23:35:48
Start date:	01/11/2021
Path:	/usr/lib/udisks2/udisksd
Arguments:	n/a
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: 5371 Parent PID: 799

General

Start time:	23:35:48
Start date:	01/11/2021
Path:	/usr/sbin/dumpe2fs
Arguments:	dumpe2fs -h /dev/sda2
File size:	31112 bytes

MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read

Analysis Process: udisksd PID: 5373 Parent PID: 799

General

Start time:	23:35:49
Start date:	01/11/2021
Path:	/usr/lib/udisks2/udisksd
Arguments:	n/a
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: 5373 Parent PID: 799

General

Start time:	23:35:49
Start date:	01/11/2021
Path:	/usr/sbin/dumpe2fs
Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read

Analysis Process: systemd PID: 5378 Parent PID: 1860

General

Start time:	23:35:59
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5378 Parent PID: 1860

General

Start time:	23:35:59
Start date:	01/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5385 Parent PID: 1

General

Start time:	23:36:03
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5385 Parent PID: 1

General

Start time:	23:36:03
Start date:	01/11/2021
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: 5400 Parent PID: 5385

General

Start time:	23:36:03
Start date:	01/11/2021
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: 5400 Parent PID: 5385

General

Start time:	23:36:04
Start date:	01/11/2021
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: 5401 Parent PID: 5400

General

Start time:	23:36:04
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5401 Parent PID: 5400

General

Start time:	23:36:04
Start date:	01/11/2021
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: 5402 Parent PID: 5401

General

Start time:	23:36:04
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes

MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5402 Parent PID: 5401

General

Start time:	23:36:04
Start date:	01/11/2021
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: 5403 Parent PID: 5402

General

Start time:	23:36:04
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5403 Parent PID: 5402

General

Start time:	23:36:04
Start date:	01/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5404 Parent PID: 5402

General

Start time:	23:36:04
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5404 Parent PID: 5402

General

Start time:	23:36:04
Start date:	01/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gdm-session-worker PID: 5386 Parent PID: 1809

General

Start time:	23:36:03
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: Default PID: 5386 Parent PID: 1809

General

Start time:	23:36:03
Start date:	01/11/2021
Path:	/etc/gdm3/PostSession/Default
Arguments:	/etc/gdm3/PostSession/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5405 Parent PID: 1320

General

Start time:	23:36:05
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5405 Parent PID: 1320

General

Start time:	23:36:05
Start date:	01/11/2021
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: 5422 Parent PID: 5405

General

Start time:	23:36:07
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 5422 Parent PID: 5405

General

Start time:	23:36:07
Start date:	01/11/2021
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

Analysis Process: gdm-wayland-session PID: 5425 Parent PID: 5422

General

Start time:	23:36:07
Start date:	01/11/2021
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: 5425 Parent PID: 5422

General

Start time:	23:36:07
Start date:	01/11/2021
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: 5426 Parent PID: 5425

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5426 Parent PID: 5425

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --nofork --print-address 4 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: dbus-daemon PID: 5430 Parent PID: 5426

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5431 Parent PID: 5430

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5431 Parent PID: 5430

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5433 Parent PID: 5426

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5434 Parent PID: 5433

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon

Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5434 Parent PID: 5433

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5435 Parent PID: 5426

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5436 Parent PID: 5435

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5436 Parent PID: 5435

General

Start time:	23:36:09

Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5437 Parent PID: 5426

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5438 Parent PID: 5437

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5438 Parent PID: 5437

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5439 Parent PID: 5426

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5440 Parent PID: 5439

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5440 Parent PID: 5439

General

Start time:	23:36:09
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5441 Parent PID: 5426

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5442 Parent PID: 5441

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon

Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5442 Parent PID: 5441

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5444 Parent PID: 5426

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5445 Parent PID: 5444

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5445 Parent PID: 5444

General

Start time:	23:36:10

Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5427 Parent PID: 5425

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5427 Parent PID: 5425

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/bin/gnome-session
Arguments:	gnome-session --autostart /usr/share/gdm/greeter/autostart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5427 Parent PID: 5425

General

Start time:	23:36:08
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	/usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

File Created

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Link Created

Analysis Process: gnome-session-binary PID: 5446 Parent PID: 5427

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: session-migration PID: 5446 Parent PID: 5427

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/bin/session-migration
Arguments:	session-migration
File size:	22680 bytes
MD5 hash:	5227af42ebf14ac2fe2acddb002f68dc

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5447 Parent PID: 5427

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5447 Parent PID: 5427

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gnome-shell PID: 5447 Parent PID: 5427

General

Start time:	23:36:10
Start date:	01/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	/usr/bin/gnome-shell
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

File Read

Directory Enumerated

Analysis Process: gdm3 PID: 5416 Parent PID: 1320

General

Start time:	23:36:05
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5416 Parent PID: 1320

General

Start time:	23:36:05
Start date:	01/11/2021
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: 5473 Parent PID: 1320

General

Start time:	23:36:14
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5473 Parent PID: 1320

General

Start time:	23:36:14
Start date:	01/11/2021
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: 5490 Parent PID: 5473

General

Start time:	23:36:16
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 5490 Parent PID: 5473

General

Start time:	23:36:16
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	/usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

File Read

File Written

Directory Created

Analysis Process: gdm-x-session PID: 5494 Parent PID: 5490

General

Start time:	23:36:17
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: Xorg PID: 5494 Parent PID: 5490

General

Start time:	23:36:17
Start date:	01/11/2021
Path:	/usr/bin/Xorg
Arguments:	/usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: Xorg.wrap PID: 5494 Parent PID: 5490

General

Start time:	23:36:17
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg.wrap
Arguments:	/usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	14488 bytes
MD5 hash:	48993830888200ecf19dd7def0884dfd

File Activities

File Read

Analysis Process: Xorg PID: 5494 Parent PID: 5490

General

Start time:	23:36:18
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	/usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Analysis Process: Xorg PID: 5506 Parent PID: 5494

General

Start time:	23:36:26
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5506 Parent PID: 5494

General

Start time:	23:36:26
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5507 Parent PID: 5506

General

Start time:	23:36:26
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5507 Parent PID: 5506

General

Start time:	23:36:26
Start date:	01/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: Xorg PID: 5752 Parent PID: 5494

General

Start time:	23:37:00
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5752 Parent PID: 5494

General

Start time:	23:37:00
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5753 Parent PID: 5752

General

Start time:	23:37:00
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5753 Parent PID: 5752

General

Start time:	23:37:00
Start date:	01/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: gdm-x-session PID: 5512 Parent PID: 5490

General

Start time:	23:36:32
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: Default PID: 5512 Parent PID: 5490

General

Start time:	23:36:32
Start date:	01/11/2021
Path:	/etc/gdm3/Prime/Default
Arguments:	/etc/gdm3/Prime/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm-x-session PID: 5513 Parent PID: 5490

General

Start time:	23:36:32
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: dbus-run-session PID: 5513 Parent PID: 5490

General

Start time:	23:36:32
Start date:	01/11/2021
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: 5514 Parent PID: 5513

General

Start time:	23:36:32
Start date:	01/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5514 Parent PID: 5513

General

Start time:	23:36:32
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --nofork --print-address 4 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: dbus-daemon PID: 5529 Parent PID: 5514

General

Start time:	23:36:40
Start date:	01/11/2021
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:	23:36:40
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: at-spi-bus-launcher PID: 5530 Parent PID: 5529

General

Start time:	23:36:40
Start date:	01/11/2021
Path:	/usr/libexec/at-spi-bus-launcher
Arguments:	/usr/libexec/at-spi-bus-launcher
File size:	27008 bytes
MD5 hash:	1563f274acd4e7ba530a55bdc4c95682

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: at-spi-bus-launcher PID: 5535 Parent PID: 5530

General

Start time:	23:36:40

Start date:	01/11/2021
Path:	/usr/libexec/at-spi-bus-launcher
Arguments:	n/a
File size:	27008 bytes
MD5 hash:	1563f274acd4e7ba530a55bdc4c95682

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 5535 Parent PID: 5530

General

Start time:	23:36:40
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5867 Parent PID: 5535

General

Start time:	23:37:03
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5868 Parent PID: 5867

General

Start time:	23:37:03
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: at-spi2-registryd PID: 5868 Parent PID: 5867

General

Start time:	23:37:03
Start date:	01/11/2021
Path:	/usr/libexec/at-spi2-registryd
Arguments:	/usr/libexec/at-spi2-registryd --use-gnome-session
File size:	100224 bytes
MD5 hash:	1d904c2693452edebc7ede3a9e24d440

File Activities

File Read

Analysis Process: dbus-daemon PID: 5559 Parent PID: 5514

General

Start time:	23:36:43
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5560 Parent PID: 5559

General

Start time:	23:36:43
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5560 Parent PID: 5559

General

Start time:	23:36:43
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5562 Parent PID: 5514

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5563 Parent PID: 5562

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5563 Parent PID: 5562

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5564 Parent PID: 5514

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5565 Parent PID: 5564

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5565 Parent PID: 5564

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5566 Parent PID: 5514

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5567 Parent PID: 5566

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5567 Parent PID: 5566

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5568 Parent PID: 5514

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5569 Parent PID: 5568

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5569 Parent PID: 5568

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5570 Parent PID: 5514

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5571 Parent PID: 5570

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5571 Parent PID: 5570

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5573 Parent PID: 5514

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5574 Parent PID: 5573

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5574 Parent PID: 5573

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5750 Parent PID: 5514

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5751 Parent PID: 5750

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: ibus-portal PID: 5751 Parent PID: 5750

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/libexec/ibus-portal
Arguments:	/usr/libexec/ibus-portal
File size:	92536 bytes
MD5 hash:	562ad55bd9a4d54bd7b76746b01e37d3

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: dbus-daemon PID: 5874 Parent PID: 5514

General

Start time:	23:37:04
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5875 Parent PID: 5874

General

Start time:	23:37:04
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: gjs PID: 5875 Parent PID: 5874

General

Start time:	23:37:04
Start date:	01/11/2021
Path:	/usr/bin/gjs
Arguments:	/usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
File size:	23128 bytes
MD5 hash:	5f3eceb792bb65c22f23d1efb4fde3ad

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5936 Parent PID: 5514

General

Start time:	23:37:20
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5937 Parent PID: 5936

General

Start time:	23:37:20
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5937 Parent PID: 5936

General

Start time:	23:37:20
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5515 Parent PID: 5513

General

Start time:	23:36:32
Start date:	01/11/2021
Path:	/usr/bin/dbus-run-session

Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5515 Parent PID: 5513

General

Start time:	23:36:33
Start date:	01/11/2021
Path:	/usr/bin/gnome-session
Arguments:	gnome-session --autostart /usr/share/gdm/greeter/autostart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5515 Parent PID: 5513

General

Start time:	23:36:33
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	/usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

File Created

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Link Created

Analysis Process: gnome-session-binary PID: 5516 Parent PID: 5515

General

Start time:	23:36:33
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5516 Parent PID: 5515

General

Start time:	23:36:33
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-check-accelerated
Arguments:	/usr/libexec/gnome-session-check-accelerated
File size:	18752 bytes
MD5 hash:	a64839518af85b2b9de31aca27646396

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5536 Parent PID: 5516

General

Start time:	23:36:40
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-check-accelerated
Arguments:	n/a
File size:	18752 bytes
MD5 hash:	a64839518af85b2b9de31aca27646396

File Activities

Directory Enumerated

Analysis Process: gnome-session-check-accelerated-gl-helper PID: 5536 Parent PID: 5516

General

Start time:	23:36:40
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-check-accelerated-gl-helper
Arguments:	/usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
File size:	22920 bytes
MD5 hash:	b1ab9a384f9e98a39ae5c36037dd5e78

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5548 Parent PID: 5516

General

Start time:	23:36:42
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-check-accelerated
Arguments:	n/a
File size:	18752 bytes
MD5 hash:	a64839518af85b2b9de31aca27646396

File Activities

Directory Enumerated

Analysis Process: gnome-session-check-accelerated-gles-helper PID: 5548 Parent PID: 5516

General

Start time:	23:36:42
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-check-accelerated-gles-helper
Arguments:	/usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
File size:	14728 bytes
MD5 hash:	1bd78885765a18e60c05ed1fb5fa3bf8

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: 5575 Parent PID: 5515

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: session-migration PID: 5575 Parent PID: 5515

General

Start time:	23:36:44
Start date:	01/11/2021
Path:	/usr/bin/session-migration

Arguments:	session-migration
File size:	22680 bytes
MD5 hash:	5227af42ebf14ac2fe2acddb002f68dc

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5576 Parent PID: 5515

General

Start time:	23:36:45
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5576 Parent PID: 5515

General

Start time:	23:36:45
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gnome-shell PID: 5576 Parent PID: 5515

General

Start time:	23:36:46
Start date:	01/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	/usr/bin/gnome-shell
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-shell PID: 5623 Parent PID: 5576

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5623 Parent PID: 5576

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	ibus-daemon --panel disable --xim
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5746 Parent PID: 5623

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5746 Parent PID: 5623

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/libexec/ibus-memconf
Arguments:	/usr/libexec/ibus-memconf
File size:	22904 bytes
MD5 hash:	523e939905910d06598e66385761a822

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5748 Parent PID: 5623

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5749 Parent PID: 5748

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5749 Parent PID: 1

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/libexec/ibus-x11

Arguments:	/usr/libexec/ibus-x11 --kill-daemon
File size:	100352 bytes
MD5 hash:	2aa1e54666191243814c2733d6992dbd

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5915 Parent PID: 5623

General

Start time:	23:37:14
Start date:	01/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-engine-simple PID: 5915 Parent PID: 5623

General

Start time:	23:37:15
Start date:	01/11/2021
Path:	/usr/libexec/ibus-engine-simple
Arguments:	/usr/libexec/ibus-engine-simple
File size:	14712 bytes
MD5 hash:	0238866d5e8802a0ce1b1b9af8cb1376

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 5890 Parent PID: 5515

General

Start time:	23:37:08
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5890 Parent PID: 5515

General

Start time:	23:37:08
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-sharing PID: 5890 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/usr/libexec/gsd-sharing
Arguments:	/usr/libexec/gsd-sharing
File size:	35424 bytes
MD5 hash:	e29d9025d98590fbb69f89fdbd4438b3

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 5892 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5892 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-wacom PID: 5892 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/usr/libexec/gsd-wacom
Arguments:	/usr/libexec/gsd-wacom
File size:	39520 bytes
MD5 hash:	13778dd1a23a4e94ddc17ac9caa4fcc1

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: 5894 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5894 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-color PID: 5894 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gsd-color
Arguments:	/usr/libexec/gsd-color
File size:	92832 bytes
MD5 hash:	ac2861ad93ce047283e8e87cefef9a19

Analysis Process: gnome-session-binary PID: 5895 Parent PID: 5515

General

Start time:	23:37:09
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5895 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-keyboard PID: 5895 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gsd-keyboard
Arguments:	/usr/libexec/gsd-keyboard
File size:	39760 bytes
MD5 hash:	8e288fd17c80bb0a1148b964b2ac2279

Analysis Process: gnome-session-binary PID: 5896 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5896 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-print-notifications PID: 5896 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6090 Parent PID: 5896

General

Start time:	23:37:24
Start date:	01/11/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6091 Parent PID: 6090

General

Start time:	23:37:24
Start date:	01/11/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-printer PID: 6091 Parent PID: 1

General

Start time:	23:37:24
Start date:	01/11/2021
Path:	/usr/libexec/gsd-printer
Arguments:	/usr/libexec/gsd-printer
File size:	31120 bytes

MD5 hash:	7995828cf98c315fd55f2ffb3b22384d

Analysis Process: gnome-session-binary PID: 5897 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5897 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-rfkill PID: 5897 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gsd-rfkill
Arguments:	/usr/libexec/gsd-rfkill
File size:	51808 bytes
MD5 hash:	88a16a3c0aba1759358c06215ecfb5cc

Analysis Process: gnome-session-binary PID: 5898 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5898 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/bin/sh

Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-smartcard PID: 5898 Parent PID: 5515

General

Start time:	23:37:11
Start date:	01/11/2021
Path:	/usr/libexec/gsd-smartcard
Arguments:	/usr/libexec/gsd-smartcard
File size:	109152 bytes
MD5 hash:	ea1fbd7f62e4cd0331eae2ef754ee605

Analysis Process: gnome-session-binary PID: 5899 Parent PID: 5515

General

Start time:	23:37:10
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5899 Parent PID: 5515

General

Start time:	23:37:11
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-datetime PID: 5899 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/usr/libexec/gsd-datetime
Arguments:	/usr/libexec/gsd-datetime
File size:	76736 bytes
MD5 hash:	d80d39745740de37d6634d36e344d4bc

Analysis Process: gnome-session-binary PID: 5903 Parent PID: 5515

General

Start time:	23:37:11

Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5903 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-media-keys PID: 5903 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/usr/libexec/gsd-media-keys
Arguments:	/usr/libexec/gsd-media-keys
File size:	232936 bytes
MD5 hash:	a425448c135afb4b8bfd79cc0b6b74da

Analysis Process: gnome-session-binary PID: 5904 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5904 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-screensaver-proxy PID: 5904 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/usr/libexec/gsd-screensaver-proxy
Arguments:	/usr/libexec/gsd-screensaver-proxy
File size:	27232 bytes
MD5 hash:	77e309450c87dceee43f1a9e50cc0d02

Analysis Process: gnome-session-binary PID: 5905 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5905 Parent PID: 5515

General

Start time:	23:37:12
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-sound PID: 5905 Parent PID: 5515

General

Start time:	23:37:13
Start date:	01/11/2021
Path:	/usr/libexec/gsd-sound
Arguments:	/usr/libexec/gsd-sound
File size:	31248 bytes
MD5 hash:	4c7d3fb993463337b4a0eb5c80c760ee

Analysis Process: gnome-session-binary PID: 5909 Parent PID: 5515

General

Start time:	23:37:13
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5909 Parent PID: 5515

General

Start time:	23:37:13
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-a11y-settings PID: 5909 Parent PID: 5515

General

Start time:	23:37:14
Start date:	01/11/2021
Path:	/usr/libexec/gsd-a11y-settings
Arguments:	/usr/libexec/gsd-a11y-settings
File size:	23056 bytes
MD5 hash:	18e243d2cf30ecee7ea89d1462725c5c

Analysis Process: gnome-session-binary PID: 5911 Parent PID: 5515

General

Start time:	23:37:14
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5911 Parent PID: 5515

General

Start time:	23:37:14
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-housekeeping PID: 5911 Parent PID: 5515

General

Start time:	23:37:14
Start date:	01/11/2021
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

Analysis Process: gnome-session-binary PID: 5914 Parent PID: 5515

General

Start time:	23:37:14
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5914 Parent PID: 5515

General

Start time:	23:37:15
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-power PID: 5914 Parent PID: 5515

General

Start time:	23:37:16
Start date:	01/11/2021
Path:	/usr/libexec/gsd-power
Arguments:	/usr/libexec/gsd-power
File size:	88672 bytes
MD5 hash:	28b8e1b43c3e7f1db6741ea1ecd978b7

Analysis Process: gnome-session-binary PID: 6417 Parent PID: 5515

General

Start time:	23:37:46
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6417 Parent PID: 5515

General

Start time:	23:37:47
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: spice-vdagent PID: 6417 Parent PID: 5515

General

Start time:	23:37:47
Start date:	01/11/2021
Path:	/usr/bin/spice-vdagent
Arguments:	/usr/bin/spice-vdagent
File size:	80664 bytes
MD5 hash:	80fb7f613aa78d1b8a229dbcf4577a9d

Analysis Process: gnome-session-binary PID: 6419 Parent PID: 5515

General

Start time:	23:37:49
Start date:	01/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6419 Parent PID: 5515

General

Start time:	23:37:49
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xbrlapi PID: 6419 Parent PID: 5515

General

Start time:	23:37:50
Start date:	01/11/2021
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5474 Parent PID: 1320

General

Start time:	23:36:14
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5474 Parent PID: 1320

General

Start time:	23:36:14
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5475 Parent PID: 1320

General

Start time:	23:36:14
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5475 Parent PID: 1320

General

Start time:	23:36:14
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gvfsd-fuse PID: 5479 Parent PID: 2038

General

Start time:	23:36:15
Start date:	01/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5479 Parent PID: 2038

General

Start time:	23:36:15
Start date:	01/11/2021
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes

MD5 hash:	576a1b135c82bdcbc97a91acea900566

Analysis Process: systemd PID: 5491 Parent PID: 1

General

Start time:	23:36:16
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5491 Parent PID: 1

General

Start time:	23:36:16
Start date:	01/11/2021
Path:	/lib/systemd/systemd-user-runtime-dir
Arguments:	/lib/systemd/systemd-user-runtime-dir stop 1000
File size:	22672 bytes
MD5 hash:	d55f4b0847f88131dbcfb07435178e54

Analysis Process: systemd PID: 5600 Parent PID: 1

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5600 Parent PID: 1

General

Start time:	23:36:58
Start date:	01/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 5761 Parent PID: 1334

General

Start time:	23:37:02
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd

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

Analysis Process: pulseaudio PID: 5761 Parent PID: 1334

General

Start time:	23:37:02
Start date:	01/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5764 Parent PID: 1

General

Start time:	23:37:02
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5764 Parent PID: 1

General

Start time:	23:37:02
Start date:	01/11/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 5940 Parent PID: 1

General

Start time:	23:37:21
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-hostnamed PID: 5940 Parent PID: 1

General

Start time:	23:37:21

Start date:	01/11/2021
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	35040 bytes
MD5 hash:	2cc8a5576629a2d5bd98e49a4b8bef65

Analysis Process: systemd PID: 6175 Parent PID: 1

General

Start time:	23:37:41
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 6175 Parent PID: 1

General

Start time:	23:37:41
Start date:	01/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 6302 Parent PID: 1

General

Start time:	23:37:42
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6302 Parent PID: 1

General

Start time:	23:37:42
Start date:	01/11/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84