
**ID:** 518884
**Sample Name:** arm
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 03:44:01
**Date:** 10/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

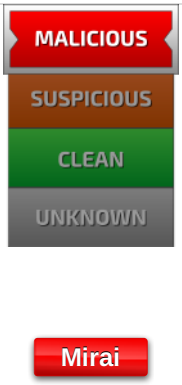
# Linux Analysis Report arm

## Overview

### General Information

| | |
|---|---|
| Sample Name: | arm |
| Analysis ID: | 518884 |
| MD5: | b31e3180a6bf96a. |
| SHA1: | ff8adee220db241.. |
| SHA256: | f693c8fe32d094d.. |
| Tags: | Mirai |
| Infos: | |

### Detection

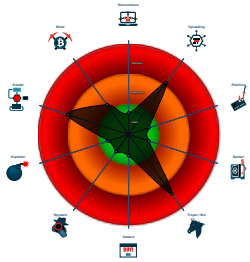



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample tries to kill many processes...
- Reads system files that contain reco...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample reads /proc/mounts (often u...
- Sample contains only a LOAD segm...
- Reads CPU information from /sys in...
- Yara signature match
- Executes the "grep" command used...

### Classification



### Analysis Advice

**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: | 518884 |
| Start date: | 10.11.2021 |
| Start time: | 03:44:01 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 10s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | arm |
| 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: | mal84.spre.troj.evad.lin@0/52@3/0 |
| Warnings: | Show All |

## Process Tree

- **system is lnxubuntu20**
- dash New Fork (PID: 5200, Parent: 4331)
  - cat (PID: 5200, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.0ZsCqe1shq
- dash New Fork (PID: 5201, Parent: 4331)
  - head (PID: 5201, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5202, Parent: 4331)
  - tr (PID: 5202, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5203, Parent: 4331)
  - cut (PID: 5203, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80

- dash New Fork (PID: 5204, Parent: 4331)
  - cat (PID: 5204, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.0ZsCqe1shq
- dash New Fork (PID: 5205, Parent: 4331)
  - head (PID: 5205, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5206, Parent: 4331)
  - tr (PID: 5206, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5207, Parent: 4331)
  - cut (PID: 5207, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5208, Parent: 4331)
  - rm (PID: 5208, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.0ZsCqe1shq /tmp/tmp.EYKo36YtKl /tmp/tmp.yzVwFZ13h1
  - arm (PID: 5255, Parent: 5105, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm
    - arm New Fork (PID: 5257, Parent: 5255)
    - arm New Fork (PID: 5259, Parent: 5255)
      - arm New Fork (PID: 5261, Parent: 5259)
      - arm New Fork (PID: 5264, Parent: 5259)
        - arm New Fork (PID: 5266, Parent: 5264)
- systemd New Fork (PID: 5303, Parent: 1)
  - whoopsie (PID: 5303, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5316, Parent: 1)
  - sshd (PID: 5316, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5317, Parent: 1)
  - sshd (PID: 5317, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5326, Parent: 1320)
  - Default (PID: 5326, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5329, Parent: 1320)
  - Default (PID: 5329, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5330, Parent: 1)
  - accounts-daemon (PID: 5330, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5348, Parent: 5330)
    - language-validate (PID: 5348, Parent: 5330, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
      - language-validate New Fork (PID: 5349, Parent: 5348)
      - language-options (PID: 5349, Parent: 5348, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
        - language-options New Fork (PID: 5350, Parent: 5349)
        - sh (PID: 5350, Parent: 5349, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
          - sh New Fork (PID: 5351, Parent: 5350)
          - locale (PID: 5351, Parent: 5350, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
          - sh New Fork (PID: 5352, Parent: 5350)
          - grep (PID: 5352, Parent: 5350, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm3 New Fork (PID: 5353, Parent: 1320)
  - gdm-session-worker (PID: 5353, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5357, Parent: 5353)
    - gdm-wayland-session (PID: 5357, Parent: 5353, 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: 5360, Parent: 5357)
      - dbus-run-session (PID: 5360, Parent: 5357, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5361, Parent: 5360)
        - dbus-daemon (PID: 5361, Parent: 5360, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
          - dbus-daemon New Fork (PID: 5367, Parent: 5361)
            - dbus-daemon New Fork (PID: 5368, Parent: 5367)
            - false (PID: 5368, Parent: 5367, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5370, Parent: 5361)
            - dbus-daemon New Fork (PID: 5371, Parent: 5370)
            - false (PID: 5371, Parent: 5370, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5372, Parent: 5361)
            - dbus-daemon New Fork (PID: 5373, Parent: 5372)
            - false (PID: 5373, Parent: 5372, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5374, Parent: 5361)
            - dbus-daemon New Fork (PID: 5375, Parent: 5374)
            - false (PID: 5375, Parent: 5374, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5376, Parent: 5361)
            - dbus-daemon New Fork (PID: 5377, Parent: 5376)
            - false (PID: 5377, Parent: 5376, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5378, Parent: 5361)
            - dbus-daemon New Fork (PID: 5379, Parent: 5378)
            - false (PID: 5379, Parent: 5378, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5381, Parent: 5361)
            - dbus-daemon New Fork (PID: 5382, Parent: 5381)
            - false (PID: 5382, Parent: 5381, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-run-session New Fork (PID: 5362, Parent: 5360)
        - gnome-session (PID: 5362, Parent: 5360, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary (PID: 5362, Parent: 5360, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
          - gnome-session-binary New Fork (PID: 5383, Parent: 5362)
          - session-migration (PID: 5383, Parent: 5362, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
          - gnome-session-binary New Fork (PID: 5384, Parent: 5362)
          - sh (PID: 5384, Parent: 5362, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
          - gnome-shell (PID: 5384, Parent: 5362, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5411, Parent: 1320)
  - gdm-session-worker (PID: 5411, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5416, Parent: 5411)
    - gdm-x-session (PID: 5416, Parent: 5411, 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: 5418, Parent: 5416)
      - Xorg (PID: 5418, Parent: 5416, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg.wrap (PID: 5418, Parent: 5416, 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: 5418, Parent: 5416, 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: 5428, Parent: 5418)
- sh (PID: 5428, Parent: 5418, 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: 5429, Parent: 5428)
  - xkbcomp (PID: 5429, Parent: 5428, 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: 5872, Parent: 5418)
- sh (PID: 5872, Parent: 5418, 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: 5873, Parent: 5872)
  - xkbcomp (PID: 5873, Parent: 5872, 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: 5462, Parent: 5416)
- Default (PID: 5462, Parent: 5416, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
- gdm-x-session New Fork (PID: 5463, Parent: 5416)
- dbus-run-session (PID: 5463, Parent: 5416, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
  - dbus-run-session New Fork (PID: 5464, Parent: 5463)
  - dbus-daemon (PID: 5464, Parent: 5463, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
    - dbus-daemon New Fork (PID: 5520, Parent: 5464)
      - dbus-daemon New Fork (PID: 5521, Parent: 5520)
      - at-spi-bus-launcher (PID: 5521, Parent: 5520, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
        - at-spi-bus-launcher New Fork (PID: 5526, Parent: 5521)
        - dbus-daemon (PID: 5526, Parent: 5521, 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: 5882, Parent: 5526)
            - dbus-daemon New Fork (PID: 5883, Parent: 5882)
            - at-spi2-registryd (PID: 5883, Parent: 5882, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
    - dbus-daemon New Fork (PID: 5549, Parent: 5464)
      - dbus-daemon New Fork (PID: 5550, Parent: 5549)
      - false (PID: 5550, Parent: 5549, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5552, Parent: 5464)
      - dbus-daemon New Fork (PID: 5553, Parent: 5552)
      - false (PID: 5553, Parent: 5552, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5554, Parent: 5464)
      - dbus-daemon New Fork (PID: 5555, Parent: 5554)
      - false (PID: 5555, Parent: 5554, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5556, Parent: 5464)
      - dbus-daemon New Fork (PID: 5557, Parent: 5556)
      - false (PID: 5557, Parent: 5556, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5558, Parent: 5464)
      - dbus-daemon New Fork (PID: 5559, Parent: 5558)
      - false (PID: 5559, Parent: 5558, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5560, Parent: 5464)
      - dbus-daemon New Fork (PID: 5561, Parent: 5560)
      - false (PID: 5561, Parent: 5560, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5563, Parent: 5464)
      - dbus-daemon New Fork (PID: 5564, Parent: 5563)
      - false (PID: 5564, Parent: 5563, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5868, Parent: 5464)
      - dbus-daemon New Fork (PID: 5869, Parent: 5868)
      - ibus-portal (PID: 5869, Parent: 5868, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
    - dbus-daemon New Fork (PID: 6091, Parent: 5464)
      - dbus-daemon New Fork (PID: 6092, Parent: 6091)
      - gjs (PID: 6092, Parent: 6091, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
    - dbus-daemon New Fork (PID: 6428, Parent: 5464)
      - dbus-daemon New Fork (PID: 6429, Parent: 6428)
      - false (PID: 6429, Parent: 6428, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-run-session New Fork (PID: 5467, Parent: 5463)
  - gnome-session (PID: 5467, Parent: 5463, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
  - gnome-session-binary (PID: 5467, Parent: 5463, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
    - gnome-session-binary New Fork (PID: 5468, Parent: 5467)
    - gnome-session-check-accelerated (PID: 5468, Parent: 5467, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
      - gnome-session-check-accelerated New Fork (PID: 5527, Parent: 5468)
      - gnome-session-check-accelerated-gl-helper (PID: 5527, Parent: 5468, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
      - gnome-session-check-accelerated New Fork (PID: 5536, Parent: 5468)
      - gnome-session-check-accelerated-gles-helper (PID: 5536, Parent: 5468, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
    - gnome-session-binary New Fork (PID: 5565, Parent: 5467)
    - session-migration (PID: 5565, Parent: 5467, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
    - gnome-session-binary New Fork (PID: 5566, Parent: 5467)
    - sh (PID: 5566, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
    - gnome-shell (PID: 5566, Parent: 5467, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
      - gnome-shell New Fork (PID: 5623, Parent: 5566)
      - ibus-daemon (PID: 5623, Parent: 5566, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
        - ibus-daemon New Fork (PID: 5864, Parent: 5623)
        - ibus-memconf (PID: 5864, Parent: 5623, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
        - ibus-daemon New Fork (PID: 5866, Parent: 5623)
          - ibus-daemon New Fork (PID: 5867, Parent: 5866)
          - ibus-x11 (PID: 5867, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
        - ibus-daemon New Fork (PID: 6133, Parent: 5623)
        - ibus-engine-simple (PID: 6133, Parent: 5623, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
    - gnome-session-binary New Fork (PID: 6110, Parent: 5467)
    - sh (PID: 6110, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
    - gsd-sharing (PID: 6110, Parent: 5467, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing

- gnome-session-binary New Fork (PID: 6112, Parent: 5467)
  - sh (PID: 6112, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
  - gsd-wacom (PID: 6112, Parent: 5467, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 6114, Parent: 5467)
  - sh (PID: 6114, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
  - gsd-color (PID: 6114, Parent: 5467, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 6115, Parent: 5467)
  - sh (PID: 6115, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
  - gsd-keyboard (PID: 6115, Parent: 5467, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 6116, Parent: 5467)
  - sh (PID: 6116, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6116, Parent: 5467, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6150, Parent: 6116)
      - gsd-print-notifications New Fork (PID: 6152, Parent: 6150)
      - gsd-printer (PID: 6152, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 6117, Parent: 5467)
  - sh (PID: 6117, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
  - gsd-rfkill (PID: 6117, Parent: 5467, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6118, Parent: 5467)
  - sh (PID: 6118, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
  - gsd-smartcard (PID: 6118, Parent: 5467, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6120, Parent: 5467)
  - sh (PID: 6120, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
  - gsd-datetime (PID: 6120, Parent: 5467, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6121, Parent: 5467)
  - sh (PID: 6121, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
  - gsd-media-keys (PID: 6121, Parent: 5467, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6126, Parent: 5467)
  - sh (PID: 6126, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
  - gsd-screensaver-proxy (PID: 6126, Parent: 5467, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6128, Parent: 5467)
  - sh (PID: 6128, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
  - gsd-sound (PID: 6128, Parent: 5467, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6130, Parent: 5467)
  - sh (PID: 6130, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
  - gsd-a11y-settings (PID: 6130, Parent: 5467, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6134, Parent: 5467)
  - sh (PID: 6134, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
  - gsd-housekeeping (PID: 6134, Parent: 5467, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6137, Parent: 5467)
  - sh (PID: 6137, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
  - gsd-power (PID: 6137, Parent: 5467, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6978, Parent: 5467)
  - sh (PID: 6978, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
  - spice-vdagent (PID: 6978, Parent: 5467, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 6981, Parent: 5467)
  - sh (PID: 6981, Parent: 5467, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
  - xbrlapi (PID: 6981, Parent: 5467, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q
- gdm3 New Fork (PID: 5412, Parent: 1320)
  - Default (PID: 5412, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5413, Parent: 1320)
  - Default (PID: 5413, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5421, Parent: 1320)
  - Default (PID: 5421, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5455, Parent: 1860)
  - pulseaudio (PID: 5455, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gvfsd-fuse New Fork (PID: 5471, Parent: 2038)
  - fusermount (PID: 5471, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5487, Parent: 1)
  - systemd-user-runtime-dir (PID: 5487, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5591, Parent: 1)
  - systemd-localed (PID: 5591, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5879, Parent: 1334)
  - pulseaudio (PID: 5879, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5884, Parent: 1)
  - geoclue (PID: 5884, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6155, Parent: 1)
  - systemd-hostnamed (PID: 6155, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6507, Parent: 1)
  - fprintd (PID: 6507, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- systemd New Fork (PID: 6715, Parent: 1)
  - systemd-localed (PID: 6715, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- **cleanup**

# Yara Overview

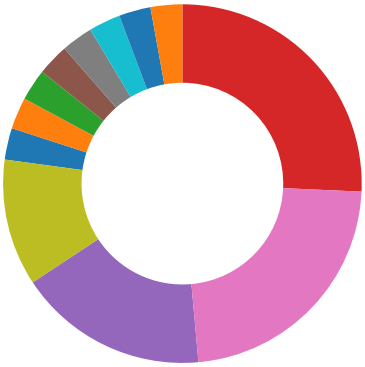
## Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| arm | SUSP_ELF_LNX_UPX_Compressed_File | Detects a suspicious ELF binary with UPX compression | Florian Roth | • 0x8e68:$s1: PROT_EXEC\|PROT_WRITE failed.<br>• 0x8ed7:$s2: $Id: UPX<br>• 0x8e88:$s3: $Info: This file is packed with the UPX executable packer |

## PCAP (Network Traffic)

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

# Jbx Signature Overview




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:

**Sample tries to kill many processes (SIGKILL)**

## Data Obfuscation:

**Sample is packed with UPX**

## Persistence and Installation Behavior:

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

## Hooking and other Techniques for Hiding and Protection:

**Uses known network protocols on non-standard ports**

## Language, Device and Operating System Detection:

**Reads system files that contain records of logged in users**

## Stealing of Sensitive Information:

**Yara detected Mirai**

## Remote Access Functionality:

**Yara detected Mirai**

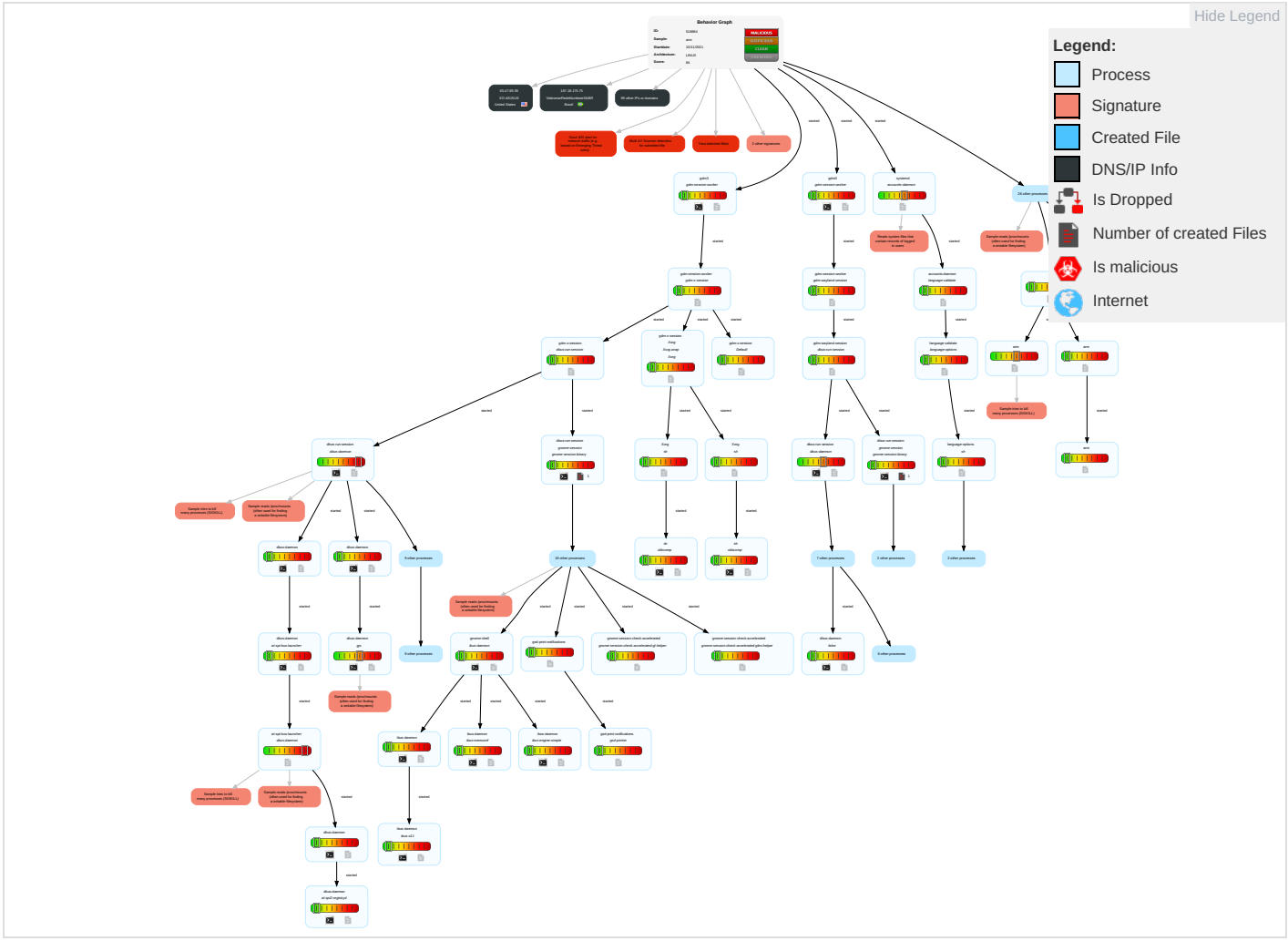
# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scripting 1 | Path Interception | Path Interception | File and Directory Permissions Modification 1 | OS Credential Dumping 1 | Security Software Discovery 1 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | M S F |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Scripting 1 | LSASS Memory | System Owner/User Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Standard Port 1 1 | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | D L |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Hidden Files and Directories 1 | Security Account Manager | File and Directory Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 1 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | D D |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 1 | NTDS | System Information Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 2 | SIM Card Swap | | C E F |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Indicator Removal on Host 1 | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | M A F F |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | File Deletion 1 | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | A A F |

# Malware Configuration

**No configs have been found**

# Behavior Graph




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| arm | 18% | Virustotal | | Browse |
| arm | 16% | ReversingLabs | Linux.Trojan.Mirai | |

## Dropped Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| daisy.ubuntu.com | 162.213.33.108 | true | false | | high |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 19.59.48.218 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 39.250.129.180 | unknown | Indonesia | | 23693 | TELKOMSEL-ASN-IDPTTelekomunikasiSelularID | false |
| 175.237.148.1 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 91.198.46.37 | unknown | Russian Federation | | 206012 | AXIOSTV-AS---UpStreams---RU | false |
| 122.191.250.25 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 206.10.220.48 | unknown | United States | | 5006 | VOYANTUS | false |
| 218.158.104.94 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 149.120.38.179 | unknown | United States | | 174 | COGENT-174US | false |
| 82.62.61.200 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 41.49.7.102 | unknown | South Africa | | 37168 | CELL-CZA | false |
| 41.78.123.10 | unknown | Central African Republic | | 22351 | INTELSAT-1US | false |
| 107.169.202.164 | unknown | Reserved | | 40676 | AS40676US | false |
| 65.47.69.39 | unknown | United States | | 2828 | XO-AS15US | false |
| 209.77.22.192 | unknown | United States | | 7132 | SBIS-ASUS | false |
| 176.53.19.93 | unknown | Turkey | | 197328 | INETLTDTR | false |
| 45.241.178.112 | unknown | Egypt | | 24863 | LINKdotNET-ASEG | false |
| 160.109.64.10 | unknown | United States | | 1294 | NTTDATA-SERVICES-AS1US | false |
| 53.148.44.7 | unknown | Germany | | 31399 | DAIMLER-ASITIGNGlobalNetworkDE | false |
| 47.99.216.211 | unknown | China | | 37963 | CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd | false |
| 133.118.225.139 | unknown | Japan | | 2522 | PPP-EXPJapanNetworkInformationCenterJP | false |
| 193.105.108.56 | unknown | United Kingdom | | 207476 | LV_IZSLV | false |
| 124.142.37.83 | unknown | Japan | | 9824 | JTCL-JP-ASJupiterTelecommunicationCoLtdJP | false |
| 98.38.68.191 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 110.76.137.58 | unknown | Australia | | 59362 | KSNETWORK-AS-APKSNetworkLimitedBD | false |
| 9.136.107.117 | unknown | United States | | 3356 | LEVEL3US | false |
| 23.169.25.13 | unknown | Reserved | | 395574 | CAMBIOBBUS | false |
| 84.73.6.176 | unknown | Switzerland | | 6830 | LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding | false |
| 4.221.60.8 | unknown | United States | | 3356 | LEVEL3US | false |
| 83.171.81.78 | unknown | Russian Federation | | 12389 | ROSTELECOM-ASRU | false |
| 159.104.120.251 | unknown | United States | | 16050 | REUTERS-DOCKLANDS-RES-ASReutersDocklandsresiliancyGB | false |
| 170.183.207.232 | unknown | United States | | 11685 | HNBCOL-ASUS | false |
| 187.18.175.75 | unknown | Brazil | | 28270 | VideomarRedeNordesteSABR | false |
| 195.65.218.77 | unknown | Switzerland | | 199642 | AS_ADUNO_2CH | false |
| 152.90.39.20 | unknown | Norway | | 21171 | SCHIBSTEDSchibstedASAAutonomoussystemOsloNorwayNO | false |
| 75.204.186.218 | unknown | United States | | 22394 | CELLCOUS | false |
| 134.190.100.180 | unknown | Canada | | 8111 | DALUNIVCA | false |
| 184.99.204.99 | unknown | United States | | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 79.103.170.149 | unknown | Greece | | 1241 | FORTHNET-GRForthnetEU | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 113.72.119.63 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 205.143.49.27 | unknown | United States | | 393341 | SPOKANE-COUNTYUS | false |
| 171.221.148.233 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 171.40.189.88 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 79.204.53.161 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 63.84.141.231 | unknown | United States | | 14414 | CROSSBRDG-ASN01US | false |
| 64.242.160.158 | unknown | United States | | 3561 | CENTURYLINK-LEGACY-SAVVISUS | false |
| 109.252.60.144 | unknown | Russian Federation | | 25513 | ASN-MGTS-USPDRU | false |
| 57.223.59.4 | unknown | Belgium | | 2686 | ATGS-MMD-ASUS | false |
| 96.162.12.219 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 109.36.132.123 | unknown | Netherlands | | 15480 | VFNL-ASVodafoneNLAutonomousSystemNL | false |
| 104.199.183.21 | unknown | United States | | 15169 | GOOGLEUS | false |
| 197.84.227.233 | unknown | South Africa | | 10474 | OPTINETZA | false |
| 216.175.40.141 | unknown | United States | | 12285 | ONE-ELEVENUS | false |
| 223.124.158.159 | unknown | China | | 58453 | CMI-INT-HKLevel30Tower1HK | false |
| 203.13.26.6 | unknown | Australia | | 2764 | AAPTAAPTLimitedAU | false |
| 132.165.52.220 | unknown | France | | 777 | CEA-SaclayEU | false |
| 97.254.245.162 | unknown | United States | | 6167 | CELLCO-PARTUS | false |
| 155.225.196.253 | unknown | United States | | 2939 | SCAROLINA-ASUS | false |
| 152.225.116.218 | unknown | United States | | 701 | UUNETUS | false |
| 59.118.62.107 | unknown | Taiwan; Republic of China (ROC) | | 3462 | HINETDataCommunicationBusinessGroupTW | false |
| 183.188.162.145 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 13.6.139.40 | unknown | United States | | 33631 | PARC-ASNUS | false |
| 200.235.176.71 | unknown | Brazil | | 1916 | AssociacaoRedeNacionaldeEnsinoePesquisaBR | false |
| 198.46.69.160 | unknown | United States | | 54290 | HOSTWINDSUS | false |
| 96.11.115.242 | unknown | United States | | 10796 | TWC-10796-MIDWESTUS | false |
| 207.46.5.115 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 165.41.215.82 | unknown | United States | | 37053 | RSAWEB-ASZA | false |
| 39.18.72.112 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 197.2.168.186 | unknown | Tunisia | | 37705 | TOPNETTN | false |
| 128.232.85.144 | unknown | United Kingdom | | 786 | JANETJiscServicesLimitedGB | false |
| 53.75.197.37 | unknown | Germany | | 31399 | DAIMLER-ASITIGNGlobalNetworkDE | false |
| 110.209.121.115 | unknown | China | | 9394 | CTTNETChinaTieTongTelecommunicationsCorporationCN | false |
| 178.129.66.47 | unknown | Russian Federation | | 28812 | JSCBIS-ASRU | false |
| 107.149.237.180 | unknown | United States | | 54600 | PEGTECHINCUS | false |
| 4.219.83.226 | unknown | United States | | 3356 | LEVEL3US | false |
| 176.197.214.42 | unknown | Russian Federation | | 39927 | ELIGHT-ASRU | false |
| 84.124.131.163 | unknown | Spain | | 6739 | ONO-ASCableuropa-ONOES | false |
| 207.58.227.111 | unknown | United States | | 22958 | FIDELITY-001US | false |
| 24.54.255.188 | unknown | Puerto Rico | | 14638 | LCPRLUS | false |
| 128.228.133.9 | unknown | United States | | 31822 | CITY-UNIVERSITY-OF-NEW-YORKUS | false |
| 118.199.26.215 | unknown | China | | 4808 | CHINA169-BJChinaUnicomBeijingProvinceNetworkCN | false |
| 5.97.10.84 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 62.44.42.143 | unknown | Germany | | 41707 | ASN-HSDG-DE | false |
| 178.230.74.165 | unknown | Netherlands | | 31615 | TMO-NL-ASNL | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 115.93.208.23 | unknown | Korea Republic of | | 3786 | LGDACOMLGDACOMCorporationKR | false |
| 187.205.197.115 | unknown | Mexico | | 8151 | UninetSAdeCVMX | false |
| 171.159.234.243 | unknown | United States | | 10794 | BANKAMERICAUS | false |
| 152.0.94.5 | unknown | Dominican Republic | | 6400 | CompaniaDominicanadeTelefonosSADO | false |
| 9.83.120.175 | unknown | United States | | 3356 | LEVEL3US | false |
| 39.163.117.41 | unknown | China | | 24445 | CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN | false |
| 70.60.131.165 | unknown | United States | | 10796 | TWC-10796-MIDWESTUS | false |
| 97.152.11.1 | unknown | United States | | 6167 | CELLCO-PARTUS | false |
| 159.140.225.169 | unknown | United States | | 17264 | CERNER-COMUS | false |
| 176.127.118.25 | unknown | Switzerland | | 3303 | SWISSCOMSwisscomSwitzerlandLtdCH | false |
| 120.3.224.35 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 12.156.59.159 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 73.107.169.67 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 185.163.151.57 | unknown | Israel | | 57259 | BROADNET-ASNIL | false |
| 175.55.216.46 | unknown | China | | 134810 | CMNET-JILIN-AS-APChinaMobileGroupJiLincommunicationsco | false |
| 181.131.145.230 | unknown | Colombia | | 13489 | EPMTelecomunicacionesSAESPCO | false |
| 191.239.1.239 | unknown | Brazil | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 45.241.178.112 | x86 | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| daisy.ubuntu.com | arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.132 |
| | Filecoder.Hive_linux.bin | Get hash | malicious | Browse | • 162.213.33.108 |
| | yFbmGHoONE | Get hash | malicious | Browse | • 162.213.33.108 |
| | zju8TB277I | Get hash | malicious | Browse | • 162.213.33.108 |
| | JYWlIP5wHP | Get hash | malicious | Browse | • 162.213.33.108 |
| | uwgXkY20gB | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.132 |
| | FWsCarsq8Q | Get hash | malicious | Browse | • 162.213.33.108 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.132 |
| | arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | 7qvn4qlmi3 | Get hash | malicious | Browse | • 162.213.33.132 |
| | JuofJwjQMT | Get hash | malicious | Browse | • 162.213.33.108 |
| | GRPVtMlbK5 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.108 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.108 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| KIXS-AS-KRKoreaTelecomKR | sora.arm | Get hash | malicious | Browse | • 211.217.82.4 |
| | KKveTTgaAAsecNNaaaa.arm | Get hash | malicious | Browse | • 39.23.193.144 |
| | v9o2vinbUj | Get hash | malicious | Browse | • 39.17.222.203 |
| | QaCRsRGMyb | Get hash | malicious | Browse | • 121.159.7.54 |
| | x86_64 | Get hash | malicious | Browse | • 14.72.253.39 |
| | arm | Get hash | malicious | Browse | • 222.109.126.151 |
| | arm6 | Get hash | malicious | Browse | • 116.205.131.201 |
| | arm5 | Get hash | malicious | Browse | • 222.105.112.87 |
| | qgxgn5fQU1 | Get hash | malicious | Browse | • 183.97.210.171 |
| | BS0Dxmu2go | Get hash | malicious | Browse | • 121.186.106.126 |
| | GB0O1NUtmJ | Get hash | malicious | Browse | • 183.118.206.44 |
| | 4DrtSJOLjr | Get hash | malicious | Browse | • 125.151.18.134 |
| | LAQh74RNEl | Get hash | malicious | Browse | • 211.39.71.34 |
| | dYgJ72oG4f | Get hash | malicious | Browse | • 1.99.144.8 |
| | Kz2SeJpaxw | Get hash | malicious | Browse | • 59.23.254.34 |
| | O4aHLhCviL | Get hash | malicious | Browse | • 121.170.35.65 |
| | skonwRkAlJ | Get hash | malicious | Browse | • 14.79.35.160 |
| | OoeA4dABtV | Get hash | malicious | Browse | • 221.154.242.40 |
| | b8xw7rKh8F | Get hash | malicious | Browse | • 218.155.160.231 |
| | mktkJhN1Fd | Get hash | malicious | Browse | • 183.124.154.123 |
| MIT-GATEWAYSUS | sora.arm | Get hash | malicious | Browse | • 19.206.131.222 |
| | KKveTTgaAAsecNNaaaa.arm | Get hash | malicious | Browse | • 19.26.188.187 |
| | mips | Get hash | malicious | Browse | • 19.44.33.246 |
| | arm6 | Get hash | malicious | Browse | • 18.38.73.10 |
| | qgxgn5fQU1 | Get hash | malicious | Browse | • 19.80.107.224 |
| | BS0Dxmu2go | Get hash | malicious | Browse | • 18.170.106.149 |
| | GB0O1NUtmJ | Get hash | malicious | Browse | • 18.44.7.53 |
| | 4DrtSJOLjr | Get hash | malicious | Browse | • 18.7.222.233 |
| | LAQh74RNEl | Get hash | malicious | Browse | • 19.201.108.84 |
| | dYgJ72oG4f | Get hash | malicious | Browse | • 18.40.250.115 |
| | O4aHLhCviL | Get hash | malicious | Browse | • 18.11.134.23 |
| | fMGehkjmPv | Get hash | malicious | Browse | • 18.42.251.87 |
| | BKyU0T5xcw | Get hash | malicious | Browse | • 18.165.74.155 |
| | skonwRkAlJ | Get hash | malicious | Browse | • 18.34.238.241 |
| | ZvUGMRqJrx | Get hash | malicious | Browse | • 19.24.137.141 |
| | P8NtIPe7f0 | Get hash | malicious | Browse | • 18.160.247.23 |
| | OoeA4dABtV | Get hash | malicious | Browse | • 19.211.216.127 |
| | gFn4iz8ygL | Get hash | malicious | Browse | • 19.228.158.223 |
| | mktkJhN1Fd | Get hash | malicious | Browse | • 19.35.144.57 |
| | Zhh51946Eq | Get hash | malicious | Browse | • 19.11.43.50 |
| TELKOMSEL-ASN-IDPTTelekomunikasiSelularID | arm6 | Get hash | malicious | Browse | • 39.237.35.121 |
| | jyTZMJKPD2 | Get hash | malicious | Browse | • 39.196.48.231 |
| | OoeA4dABtV | Get hash | malicious | Browse | • 39.209.226.105 |
| | pZvr71PT9v | Get hash | malicious | Browse | • 39.221.88.153 |
| | cpnO27Hi5Q | Get hash | malicious | Browse | • 39.198.187.9 |
| | 7L38cWaJpW | Get hash | malicious | Browse | • 39.203.239.235 |
| | 62G7F4Mgt0 | Get hash | malicious | Browse | • 39.199.110.45 |
| | rXFu2DZdQq | Get hash | malicious | Browse | • 39.235.30.120 |
| | rMwxCtXmuJ | Get hash | malicious | Browse | • 182.0.167.151 |
| | fukfKHAGMe | Get hash | malicious | Browse | • 39.239.180.71 |
| | uV1rj8v43F | Get hash | malicious | Browse | • 39.192.36.97 |
| | mL883e3xGw | Get hash | malicious | Browse | • 39.212.244.121 |
| | B94t90Yyoz | Get hash | malicious | Browse | • 39.206.145.166 |
| | sora.x86 | Get hash | malicious | Browse | • 39.222.174.221 |
| | sora.x86 | Get hash | malicious | Browse | • 39.221.88.106 |
| | sora.arm7 | Get hash | malicious | Browse | • 39.192.245.80 |
| | sora.arm7 | Get hash | malicious | Browse | • 182.3.113.159 |
| | 8PRjJeUifB | Get hash | malicious | Browse | • 39.203.199.128 |
| | SZAYTvvY9Y | Get hash | malicious | Browse | • 182.8.245.166 |
| | ENYxttDmO1 | Get hash | malicious | Browse | • 39.240.223.231 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 8662467bc96db2d387755570446a7946 | Filecoder.Hive_linux.bin | Get hash | malicious | Browse | • 162.213.33.132 |
| | mirai.arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | 2j7dEG022b | Get hash | malicious | Browse | • 162.213.33.132 |
| | sora.arm7 | Get hash | malicious | Browse | • 162.213.33.132 |
| | sora.x86 | Get hash | malicious | Browse | • 162.213.33.132 |
| | sora.arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | EHqBakwhNU | Get hash | malicious | Browse | • 162.213.33.132 |
| | vq0sPlNJDK | Get hash | malicious | Browse | • 162.213.33.132 |
| | w07UCYGzBe | Get hash | malicious | Browse | • 162.213.33.132 |
| | Rry5mHEWuH | Get hash | malicious | Browse | • 162.213.33.132 |
| | ofgE8wetW4 | Get hash | malicious | Browse | • 162.213.33.132 |
| | 0bqzNIp9PV | Get hash | malicious | Browse | • 162.213.33.132 |
| | yjJXz4a3u6 | Get hash | malicious | Browse | • 162.213.33.132 |
| | g3wyMOTecE | Get hash | malicious | Browse | • 162.213.33.132 |
| | 7k6FKvDl0x | Get hash | malicious | Browse | • 162.213.33.132 |
| | KSzA1ujvlV | Get hash | malicious | Browse | • 162.213.33.132 |
| | y66dLhUn0G | Get hash | malicious | Browse | • 162.213.33.132 |
| | 5j9ZIHs8fD | Get hash | malicious | Browse | • 162.213.33.132 |
| | 1isequal9.arm7 | Get hash | malicious | Browse | • 162.213.33.132 |
| | 1isequal9.x86 | Get hash | malicious | Browse | • 162.213.33.132 |

## Dropped Files

| No context |
|---|

# Created / dropped Files

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

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

| /home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source | |
|---|---|
| Preview: | auto_null.monitor. |

| /proc/5317/oom_score_adj | |
|---|---|
| Process: | /usr/sbin/sshd |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 6 |
| Entropy (8bit): | 1.7924812503605778 |
| Encrypted: | false |
| SSDEEP: | 3:ptn:Dn |
| MD5: | CBF282CC55ED0792C33D10003D1F760A |
| SHA1: | 007DD8BD75468E6B7ABA4285E9B267202C7EAEED |
| SHA-256: | FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22 |
| SHA-512: | 4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC<br>0 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | -1000. |

| /proc/5368/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<br>99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5371/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<br>99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5373/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 |

| /proc/5373/oom_score_adj | |
|---|---|
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5375/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5377/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5379/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5382/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |

| /proc/5382/oom_score_adj | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5521/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5550/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5553/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5555/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |

| /proc/5555/oom_score_adj | |
|---|---|
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5557/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5559/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5561/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5564/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |

| /proc/5564/oom_score_adj | |
|---|---|
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5869/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5883/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/6092/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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/6429/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |

| /proc/6429/oom_score_adj | |
|---|---|
| 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<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /run/sshd.pid | |
|---|---|
| Process: | /usr/sbin/sshd |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 2.321928094887362 |
| Encrypted: | false |
| SSDEEP: | 3:DUc:3 |
| MD5: | 3464AA45932E8B6C43906DD27DECD892 |
| SHA1: | 3DBF53863A9D9308DA2250E2CF1931F1E6D21F96 |
| SHA-256: | 3C1DACA8B1C7BBA79E5E56D3033A58521BEC1DB1731F8DEC527760165F7483DF |
| SHA-512: | 2F9054AE0D74F5ADB703FC78500CF17A024D8EE5C7692B8BFFF50B5D810E2D0448A1781485109F62A03D9C11F4846096F56CE70BD82A553D40C626C75331AD7( |
| Malicious: | false |
| Preview: | <br>5317. |

| /run/user/1000/pulse/pid | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 1.3709505944546687 |
| Encrypted: | false |
| SSDEEP: | 3:EV:EV |
| MD5: | B0819B8CE0B3868B0308B95E94CBFB37 |
| SHA1: | 583BE8C77A0E79A2506F350961DBED71FE540D36 |
| SHA-256: | 0219AAF9F1644A9A5B589DBD474D773BCBA7664E4C032E960C57389B4A09F96A |
| SHA-512: | 4ACC72BC18BFBB7DD7585465C76EEE7A7BD6777DCA6406C709D8B8B696CFAD0B6C39AE86D18C89027B794217788FB5A6E31324757EFCA502FF849B708E2BC4<br>B1 |
| Malicious: | false |
| Preview: | <br>5455. |

| /run/user/127/ICEauthority | |
|---|---|
| Process: | /usr/libexec/gnome-session-binary |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1304 |
| Entropy (8bit): | 6.033101627291036 |
| Encrypted: | false |
| SSDEEP: | 12:OxP3u2PveY+3uvAMqyxP8QOzJOveY+84kzxP5mhijveY+5tWmxPwWoveY+wcZVvJ:UfEytOlA7wqrPAIJcN |
| MD5: | 8C4E4555DD5F12DDE86880AC6BCBE207 |
| SHA1: | EB2E6A6F5BFB07AB93EC8E42A508AB04637E05CD |
| SHA-256: | 0207005CE8FA2D37F29AC7B87F34C81BAC038BCAB2060702886285A57C6DB294 |
| SHA-512: | F6676E4B06B9EA7C84128CBC457778CD5AE14165857BC541ADAC280A0B92DA1F9AC801AA203659AB6BE692BBFC0A0D6022A9CAA298D37E50375598E3D6F94D<br>F1 |
| Malicious: | false |

| /run/user/127/ICEauthority | |
|---|---|
| Preview: | ..XSMP...!unix/galassia:/tmp/.ICE-unix/5467..MIT-MAGIC-COOKIE-1.....e..."8}m..E.7..XSMP...#local/galassia:@/tmp/.ICE-unix/5467..MIT-MAGIC-COOKIE-1....dp~..%$.....ICE...!unix/galassia:/tmp/.ICE-unix/5362..MIT-MAGIC-COOKIE-1....0'..S[b.~*.....ICE...#local/galassia:@/tmp/.ICE-unix/5362..MIT-MAGIC-COOKIE-1....(.....Ek.a;R...XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.....A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....o.(R...}.9...ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'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 |
| Size (bytes): | 104 |
| Entropy (8bit): | 4.944833248737334 |
| Encrypted: | false |
| SSDEEP: | 3:rg/WFllasO93pGAPitWFllasO93pGAPi9:rg/WFl25GTWFl25GH |
| MD5: | EA979BEE1075891F5733F4B0C0309F04 |
| SHA1: | 773618497E653908AE838E76961EE36F57962567 |
| SHA-256: | 28EF07491182543EBD581C2787B659281628D536F0D5B306D8759FADB666CD94 |
| SHA-512: | 3EE12DE9822DE4968BECA0A58FE2C909AC8532C161E0D313B32F898CA774C7CC74F14B9195691BFF3A0D5CF40C5C2D35BDCD01C7EDCE33FFD7A90F0BC43BCE3 |
| Malicious: | false |
| Preview: | ....galassia....MIT-MAGIC-COOKIE-1..m5.}.%j\.nm..~.....galassia....MIT-MAGIC-COOKIE-1..m5.}.%j\.nm..~. |

| /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:Ivv:Ivv |
| MD5: | C7B66FB9C2EBE5274E1EDCD3D26D2431 |
| SHA1: | C24A04AA713BA2E321BC7EFF1CAF5B487609E152 |
| SHA-256: | 1A70833789D66610A535470830C3B41442B307B233AB23B38847B2A826847F01 |
| SHA-512: | 0AA9BA9D69E4C326FFEA5F56CCF4C6FEB8C576A89B1644C60AC89F78F5AD7C689C56DC773A179AFAA475E256E6FAD8BABB6E6CF5A77608A09A43DE0F343F6375 |
| Malicious: | false |
| Preview: | 5879. |

| /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 |

| /tmp/server-0.xkm | |
|---|---|
| SHA1: | 7D35426357695EBA77850757E8939A62DCEFF2D1 |
| SHA-256: | 7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91 |
| SHA-512: | 8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE0<br>1 |
| Malicious: | false |
| Preview: | .mkx.....D.....h.....<.....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta<br>....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD<br>06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB<br>08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP<br>3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWN<br>PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI<br>NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181<br>I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18 |

| /var/cache/motd-news | |
|---|---|
| Process: | /usr/bin/cut |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 191 |
| Entropy (8bit): | 4.515771857099866 |
| Encrypted: | false |
| SSDEEP: | 3:P2lnI+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn |
| MD5: | DD514F892B5F93ED615D366E58AC58AF |
| SHA1: | BA75EDB3C2232CC260BC187F604DC8F25AA72C11 |
| SHA-256: | F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF |
| SHA-512: | 9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACCDBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42A<br>2D0 |
| Malicious: | false |
| Preview: | * Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation. |

| /var/lib/AccountsService/users/gdm.120LC1 | |
|---|---|
| Process: | /usr/lib/accountsservice/accounts-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 61 |
| Entropy (8bit): | 4.66214589518167 |
| Encrypted: | false |
| SSDEEP: | 3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M |
| MD5: | 542BA3FB41206AE43928AF1C5E61FEBC |
| SHA1: | F56F574DAF50D609526B36B5B54FDD59EA4D6A26 |
| SHA-256: | 730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A |
| SHA-512: | D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F<br>AEA |
| Malicious: | false |
| Preview: | [User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true. |

| /var/lib/AccountsService/users/gdm.NWB7B1 | |
|---|---|
| Process: | /usr/lib/accountsservice/accounts-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 61 |
| Entropy (8bit): | 4.66214589518167 |
| Encrypted: | false |
| SSDEEP: | 3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M |
| MD5: | 542BA3FB41206AE43928AF1C5E61FEBC |
| SHA1: | F56F574DAF50D609526B36B5B54FDD59EA4D6A26 |
| SHA-256: | 730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A |
| SHA-512: | D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F<br>AEA |
| Malicious: | false |
| Preview: | [User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true. |

| /var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0 | |
|---|---|
| Process: | /usr/bin/ibus-daemon |

| /var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0 | |
|---|---|
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 381 |
| Entropy (8bit): | 5.140478984778867 |
| Encrypted: | false |
| SSDEEP: | 6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWaGgFs5x41V:q5sU3LWfLUDmQymqSFbfomSQfFsMfD |
| MD5: | ACADDA30E8B9EC30F1D2378433410145 |
| SHA1: | 3E47E696D4920442999A89BFF9BBC11D65357EC2 |
| SHA-256: | AB1ED58C200DB4E7CDD4D4955DB742A25C34C1EF834612A067091272F7AAC7BE |
| SHA-512: | 1241CCFFBB31D31A532152BF498D3F4286607EA600F6F77A4F0866720CF335F92DDBC57589815B23B9EE20F42F365E75EDD298D1961A4EC32BBE8ED16BDBA86 |
| 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-OoBJDqbO,guid=dd5c0481c44edb80fea755d6618b4095.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 |
| SHA-512: | BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09 |
| 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: | BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09 |
| Malicious: | false |
| Preview: | . |

| /var/lib/whoopsie/whoopsie-id.SM0OC1 | |
|---|---|
| Process: | /usr/bin/whoopsie |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 128 |
| Entropy (8bit): | 3.9410969045919657 |
| Encrypted: | false |
| SSDEEP: | 3:19y6UTAvBTdDVEQcNgAT0XUQhd3tjCZccCKcsVQWQ7JW:3y6BlVEfQXU8djCZd40 |
| MD5: | D2B5AAF22916F8D6665CF9E835EAD5E7 |
| SHA1: | AAEF3CE527B8F1E3733BCD03EF7A6C0F30881E15 |
| SHA-256: | FEB925D4465BF6D30A42B19112406AD1B59BA90673DC4F91B25005A90FEFEB36 |
| SHA-512: | B55A45FA0DECE5A3B0348BC3F3031A7329590E57BAD5013690AFEAA9825C0DE4B75D27057A56C33800F1626935840DA2262AAF14E795C75F39362B728D95F18A |
| Malicious: | false |
| Preview: | 9aadafe2051348cd32033e1cad68f0a5fe46fba3240ac1e6e42158f31b8a1371790c09baf3996b4979fe8e533446c7dedf30f654c68b25357334c66911dc6a9e |

| /var/log/Xorg.0.log | |
|---|---|
| Process: | /usr/lib/xorg/Xorg |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 41347 |
| Entropy (8bit): | 5.287418776373432 |
| Encrypted: | false |
| SSDEEP: | 384:HjqbYzyKRlBMadudadcdKdNdldXd8dzdXd0dBdbd4dwdydIdCdWdkdy0dGzdjEdR:Dq0tRk4m5BGgLnFoGcRaH |
| MD5: | 6993108A019300B64B5837773E45A742 |
| SHA1: | 7774BE47351C1D88FE54631D1695C2E72D0DF8F3 |
| SHA-256: | A6CDA3A16B803ABD014FBF49D98841A62F79BFD5B5DA020F36A13D4B099FAE2F |
| SHA-512: | BC66B25A951754697482E3CF79E62A29DC4DB490B9D7418AAA90E4CB5FEACB973B57B34B96F1EEFA8B4B9CA2680B80549BC26E7B6B269CAA2E2126E136CE5AF4 |
| Malicious: | false |
| Preview: | [ 478.406] (--) Log file renamed from "/var/log/Xorg.pid-5418.log" to "/var/log/Xorg.0.log".[ 478.428] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[ 478.438] Build Operating System: linux Ubuntu.[ 478.443] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[ 478.449] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[ 478.465] Build Date: 06 July 2021 10:17:51AM.[ 478.470] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[ 478.475] Current version of pixman: 0.38.4.[ 478.480] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[ 478.485] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??) |

# Static File Info

## General

| | |
|---|---|
| File type: | ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped |
| Entropy (8bit): | 7.964798540868149 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | arm |
| File size: | 38460 |
| MD5: | b31e3180a6bf96af79f2b181a494d87f |
| SHA1: | ff8adee220db2416071830ff02f8ea64e13bd4ef |
| SHA256: | f693c8fe32d094d0b6ae8f4d68d8f98789d8c57e997b1f4ba0163587d150f27e |
| SHA512: | 2b1c12729b8a8b4deaa48c50db87d044e377a77b8c3215cfcda6c5017e7c44f14cdb2c500a7ad6d2be50c64ddb6df30a09c5c3f07a5d573277aa9e7266c145c |
| SSDEEP: | 768:NFFDuUbk6s2BrnLDwzmS7ps5k/oNLHPuv9JduU7psUcxDqs3Uozwk+:LZJQ6s25Lc6S7e5kOD+9JkU7pFcdza |
| File Content Preview: | .ELF...a.....(.....4.....4. ...(.....G...G.....(.....Q.td.....UPX!.....E...E.....R.....?.E.h;.}...^.....e.&.3n....._.@..J.... .....z.G.q.....bZP.F.~io |

## Static ELF Info

| ELF header | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, little endian |
| Version: | 1 (current) |
| Machine: | ARM |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | ARM - ABI |
| ABI Version: | 0 |
| Entry Point Address: | 0x10398 |
| Flags: | 0x202 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 0 |
| Section Header Size: | 40 |
| Number of Section Headers: | 0 |

### ELF header

| | |
|---|---|
| Header String Table Index: | 0 |

### Program Segments

| Type | Offset | Virtual Address | Physical Address | File Size | Memory Size | Entropy | Flags | Flags Description | Align | Prog Interpreter | Section Mappings |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LOAD | 0x0 | 0x8000 | 0x8000 | 0x9547 | 0x9547 | 4.0247 | 0x5 | R E | 0x8000 | | |
| LOAD | 0x28ac | 0x2a8ac | 0x2a8ac | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x8000 | | |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

# Network Behavior

## TCP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 10, 2021 03:45:24.916140079 CET | 192.168.2.23 | 1.1.1.1 | 0xf59 | Standard query (0) | daisy.ubuntu.com | A (IP address) | IN (0x0001) |
| Nov 10, 2021 03:45:24.916378021 CET | 192.168.2.23 | 1.1.1.1 | 0xf7e5 | Standard query (0) | daisy.ubuntu.com | 28 | IN (0x0001) |
| Nov 10, 2021 03:45:25.033551931 CET | 192.168.2.23 | 1.1.1.1 | 0xdb75 | Standard query (0) | daisy.ubuntu.com | 28 | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 10, 2021 03:45:24.943732977 CET | 1.1.1.1 | 192.168.2.23 | 0xf59 | No error (0) | daisy.ubuntu.com | | 162.213.33.108 | A (IP address) | IN (0x0001) |
| Nov 10, 2021 03:45:24.943732977 CET | 1.1.1.1 | 192.168.2.23 | 0xf59 | No error (0) | daisy.ubuntu.com | | 162.213.33.132 | A (IP address) | IN (0x0001) |

# System Behavior

## Analysis Process: dash PID: 5200 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: cat PID: 5200 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cat |
| Arguments: | cat /tmp/tmp.0ZsCqe1shq |
| File size: | 43416 bytes |
| MD5 hash: | 7e9d213e404ad3bb82e4ebb2e1f2c1b3 |

### File Activities

#### File Read

## Analysis Process: dash PID: 5201 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: head PID: 5201 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/head |
| Arguments: | head -n 10 |
| File size: | 47480 bytes |
| MD5 hash: | fd96a67145172477dd57131396fc9608 |

### File Activities

#### File Read

## Analysis Process: dash PID: 5202 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: tr PID: 5202 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/tr |
| Arguments: | tr -d \\000-\\011\\013\\014\\016-\\037 |
| File size: | 51544 bytes |
| MD5 hash: | fbd1402dd9f72d8ebfff00ce7c3a7bb5 |

### File Activities

File Read

## Analysis Process: dash PID: 5203 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: cut PID: 5203 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cut |
| Arguments: | cut -c -80 |
| File size: | 47480 bytes |
| MD5 hash: | d8ed0ea8f22c0de0f8692d4d9f1759d3 |

### File Activities

File Read

## Analysis Process: dash PID: 5204 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: cat PID: 5204 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cat |
| Arguments: | cat /tmp/tmp.0ZsCqe1shq |
| File size: | 43416 bytes |
| MD5 hash: | 7e9d213e404ad3bb82e4ebb2e1f2c1b3 |

### File Activities

File Read

## Analysis Process: dash PID: 5205 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: head PID: 5205 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/head |
| Arguments: | head -n 10 |
| File size: | 47480 bytes |
| MD5 hash: | fd96a67145172477dd57131396fc9608 |

### File Activities

#### File Read

## Analysis Process: dash PID: 5206 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: tr PID: 5206 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/tr |
| Arguments: | tr -d \\000-\\011\\013\\014\\016-\\037 |
| File size: | 51544 bytes |
| MD5 hash: | fbd1402dd9f72d8ebfff00ce7c3a7bb5 |

### File Activities

#### File Read

## Analysis Process: dash PID: 5207 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: cut PID: 5207 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cut |
| Arguments: | cut -c -80 |
| File size: | 47480 bytes |
| MD5 hash: | d8ed0ea8f22c0de0f8692d4d9f1759d3 |

### File Activities

#### File Read

#### File Written

## Analysis Process: dash PID: 5208 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: rm PID: 5208 Parent PID: 4331

### General

| | |
|---|---|
| Start time: | 03:44:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/rm |
| Arguments: | rm -f /tmp/tmp.0ZsCqe1shq /tmp/tmp.EYKo36YtKl /tmp/tmp.yzVwFZ13h1 |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

### File Activities

#### File Deleted

#### File Read

## Analysis Process: arm PID: 5255 Parent PID: 5105

### General

| | |
|---|---|
| Start time: | 03:44:41 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm |
| Arguments: | /tmp/arm |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

#### File Read

## Analysis Process: arm PID: 5257 Parent PID: 5255

### General

| | |
|---|---|
| Start time: | 03:44:42 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: arm PID: 5259 Parent PID: 5255

### General

| | |
|---|---|
| Start time: | 03:44:42 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: arm PID: 5261 Parent PID: 5259

### General

| | |
|---|---|
| Start time: | 03:44:42 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: arm PID: 5264 Parent PID: 5259

### General

| | |
|---|---|
| Start time: | 03:44:42 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: arm PID: 5266 Parent PID: 5264

### General

| | |
|---|---|
| Start time: | 03:44:42 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: systemd PID: 5303 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: whoopsie PID: 5303 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/whoopsie |
| Arguments: | /usr/bin/whoopsie -f |
| File size: | 68592 bytes |
| MD5 hash: | d3a6915d0e7398fb4c89a037c13959c8 |

### File Activities

#### File Read

#### File Written

#### File Moved

#### Directory Enumerated

#### Directory Created

Permission Modified

## Analysis Process: systemd PID: 5316 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: sshd PID: 5316 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/sshd |
| Arguments: | /usr/sbin/sshd -t |
| File size: | 876328 bytes |
| MD5 hash: | dbca7a6bbf7bf57fedac243d4b2cb340 |

### File Activities

File Read

Directory Enumerated

## Analysis Process: systemd PID: 5317 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: sshd PID: 5317 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/sshd |
| Arguments: | /usr/sbin/sshd -D |
| File size: | 876328 bytes |
| MD5 hash: | dbca7a6bbf7bf57fedac243d4b2cb340 |

### File Activities

### File Read

### File Written

### Directory Enumerated

## Analysis Process: gdm3 PID: 5326 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5326 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| 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: 5329 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5329 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: systemd PID: 5330 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: accounts-daemon PID: 5330 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/accountsservice/accounts-daemon |
| Arguments: | /usr/lib/accountsservice/accounts-daemon |
| File size: | 203192 bytes |
| MD5 hash: | 01a899e3fb5e7e434bea1290255a1f30 |

### File Activities

#### File Read

#### File Written

#### File Moved

#### Directory Enumerated

#### Directory Created

#### Permission Modified

## Analysis Process: accounts-daemon PID: 5348 Parent PID: 5330

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| 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: 5348 Parent PID: 5330

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| 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: 5349 Parent PID: 5348

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| Path: | /usr/share/language-tools/language-validate |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: language-options PID: 5349 Parent PID: 5348

### General

| | |
|---|---|
| Start time: | 03:45:35 |
| Start date: | 10/11/2021 |
| 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: 5350 Parent PID: 5349

### General

| | |
|---|---|
| Start time: | 03:45:36 |
| Start date: | 10/11/2021 |
| Path: | /usr/share/language-tools/language-options |
| Arguments: | n/a |
| File size: | 3478464 bytes |
| MD5 hash: | 16a21f464119ea7fad1d3660de963637 |

## Analysis Process: sh PID: 5350 Parent PID: 5349

### General

| | |
|---|---|
| Start time: | 03:45:36 |
| Start date: | 10/11/2021 |
| 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: 5351 Parent PID: 5350

### General

| | |
|---|---|
| Start time: | 03:45:36 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: locale PID: 5351 Parent PID: 5350

### General

| | |
|---|---|
| Start time: | 03:45:36 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/locale |
| Arguments: | locale -a |
| File size: | 58944 bytes |
| MD5 hash: | c72a78792469db86d91369c9057f20d2 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: sh PID: 5352 Parent PID: 5350

### General

| | |
|---|---|
| Start time: | 03:45:36 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: grep PID: 5352 Parent PID: 5350

### General

| | |
|---|---|
| Start time: | 03:45:36 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/grep |
| Arguments: | grep -F .utf8 |
| File size: | 199136 bytes |
| MD5 hash: | 1e6ebb9dd094f774478f72727bdba0f5 |

### File Activities

#### File Read

## Analysis Process: gdm3 PID: 5353 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: gdm-session-worker PID: 5353 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:37 |
| Start date: | 10/11/2021 |
| 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: 5357 Parent PID: 5353

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

## Analysis Process: gdm-wayland-session PID: 5357 Parent PID: 5353

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| 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: 5360 Parent PID: 5357

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| 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: 5360 Parent PID: 5357

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| 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: 5361 Parent PID: 5360

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: dbus-daemon PID: 5361 Parent PID: 5360

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| 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: 5367 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5368 Parent PID: 5367

### General

| | |
|---|---|
| Start time: | 03:45:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5368 Parent PID: 5367

### General

| | |
|---|---|
| Start time: | 03:45:40 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |

| | |
|---|---|
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5370 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5371 Parent PID: 5370

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5371 Parent PID: 5370

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5372 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |

| | |
|---|---|
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5373 Parent PID: 5372

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5373 Parent PID: 5372

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5374 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5375 Parent PID: 5374

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |

| | |
|---|---|
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5375 Parent PID: 5374

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5376 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5377 Parent PID: 5376

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5377 Parent PID: 5376

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |

| | |
|---|---|
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5378 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5379 Parent PID: 5378

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5379 Parent PID: 5378

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5381 Parent PID: 5361

### General

| | |
|---|---|
| Start time: | 03:45:41 |

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

## Analysis Process: dbus-daemon PID: 5382 Parent PID: 5381

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5382 Parent PID: 5381

### General

| | |
|---|---|
| Start time: | 03:45:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-run-session PID: 5362 Parent PID: 5360

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: gnome-session PID: 5362 Parent PID: 5360

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| 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: 5362 Parent PID: 5360

### General

| | |
|---|---|
| Start time: | 03:45:39 |
| Start date: | 10/11/2021 |
| 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: 5383 Parent PID: 5362

### General

| | |
|---|---|
| Start time: | 03:45:42 |
| Start date: | 10/11/2021 |
| 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: 5383 Parent PID: 5362

### General

| | |
|---|---|
| Start time: | 03:45:42 |
| Start date: | 10/11/2021 |

| | |
|---|---|
| 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: 5384 Parent PID: 5362

### General

| | |
|---|---|
| Start time: | 03:45:43 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

##### Directory Enumerated

## Analysis Process: sh PID: 5384 Parent PID: 5362

### General

| | |
|---|---|
| Start time: | 03:45:43 |
| Start date: | 10/11/2021 |
| 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: 5384 Parent PID: 5362

### General

| | |
|---|---|
| Start time: | 03:45:43 |
| Start date: | 10/11/2021 |
| 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: 5411 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: gdm-session-worker PID: 5411 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:47 |
| Start date: | 10/11/2021 |
| 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: 5416 Parent PID: 5411

### General

| | |
|---|---|
| Start time: | 03:45:48 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

## Analysis Process: gdm-x-session PID: 5416 Parent PID: 5411

### General

| | |
|---|---|
| Start time: | 03:45:48 |
| Start date: | 10/11/2021 |
| 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: 5418 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:45:48 |
| Start date: | 10/11/2021 |
| 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: 5418 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:45:48 |
| Start date: | 10/11/2021 |
| 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: 5418 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:45:48 |
| Start date: | 10/11/2021 |
| 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: 5418 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:45:48 |
| Start date: | 10/11/2021 |
| 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: 5428 Parent PID: 5418

### General

| | |
|---|---|
| Start time: | 03:45:57 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | n/a |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

## Analysis Process: sh PID: 5428 Parent PID: 5418

### General

| | |
|---|---|
| Start time: | 03:45:57 |
| Start date: | 10/11/2021 |
| 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: 5429 Parent PID: 5428

### General

| | |
|---|---|
| Start time: | 03:45:57 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: xkbcomp PID: 5429 Parent PID: 5428

### General

| | |
|---|---|
| Start time: | 03:45:57 |
| Start date: | 10/11/2021 |
| 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: 5872 Parent PID: 5418

### General

| | |
|---|---|
| Start time: | 03:46:30 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | n/a |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

## Analysis Process: sh PID: 5872 Parent PID: 5418

### General

| | |
|---|---|
| Start time: | 03:46:30 |
| Start date: | 10/11/2021 |
| 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: 5873 Parent PID: 5872

### General

| | |
|---|---|
| Start time: | 03:46:30 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |

| | |
|---|---|
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: xkbcomp PID: 5873 Parent PID: 5872

### General

| | |
|---|---|
| Start time: | 03:46:30 |
| Start date: | 10/11/2021 |
| 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: 5462 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:46:04 |
| Start date: | 10/11/2021 |
| 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: 5462 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:46:04 |
| Start date: | 10/11/2021 |
| 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: 5463 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:46:04 |
| Start date: | 10/11/2021 |
| 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: 5463 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 03:46:04 |
| Start date: | 10/11/2021 |
| 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: 5464 Parent PID: 5463

### General

| | |
|---|---|
| Start time: | 03:46:04 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: dbus-daemon PID: 5464 Parent PID: 5463

### General

| | |
|---|---|
| Start time: | 03:46:04 |
| Start date: | 10/11/2021 |
| 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: 5520 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:13 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5521 Parent PID: 5520

### General

| | |
|---|---|
| Start time: | 03:46:13 |
| Start date: | 10/11/2021 |
| 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: 5521 Parent PID: 5520

### General

| | |
|---|---|
| Start time: | 03:46:13 |
| Start date: | 10/11/2021 |
| 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: 5526 Parent PID: 5521

### General

| | |
|---|---|
| Start time: | 03:46:13 |

| | |
|---|---|
| Start date: | 10/11/2021 |
| 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: 5526 Parent PID: 5521

#### General

| | |
|---|---|
| Start time: | 03:46:13 |
| Start date: | 10/11/2021 |
| 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: 5882 Parent PID: 5526

#### General

| | |
|---|---|
| Start time: | 03:46:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5883 Parent PID: 5882

#### General

| | |
|---|---|
| Start time: | 03:46:32 |
| Start date: | 10/11/2021 |
| 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: 5883 Parent PID: 5882

### General

| | |
|---|---|
| Start time: | 03:46:32 |
| Start date: | 10/11/2021 |
| 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: 5549 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:15 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5550 Parent PID: 5549

### General

| | |
|---|---|
| Start time: | 03:46:15 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5550 Parent PID: 5549

### General

| | |
|---|---|
| Start time: | 03:46:15 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5552 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:15 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5553 Parent PID: 5552

### General

| | |
|---|---|
| Start time: | 03:46:15 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5553 Parent PID: 5552

### General

| | |
|---|---|
| Start time: | 03:46:15 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5554 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5555 Parent PID: 5554

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5555 Parent PID: 5554

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5556 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5557 Parent PID: 5556

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5557 Parent PID: 5556

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5558 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5559 Parent PID: 5558

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5559 Parent PID: 5558

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5560 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5561 Parent PID: 5560

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5561 Parent PID: 5560

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5563 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5564 Parent PID: 5563

### General

| | |
|---|---|
| Start time: | 03:46:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5564 Parent PID: 5563

### General

| | |
|---|---|
| Start time: | 03:46:17 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5868 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5869 Parent PID: 5868

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: ibus-portal PID: 5869 Parent PID: 5868

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| 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: 6091 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:34 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 6092 Parent PID: 6091

### General

| | |
|---|---|
| Start time: | 03:46:34 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: gjs PID: 6092 Parent PID: 6091

### General

| | |
|---|---|
| Start time: | 03:46:34 |
| Start date: | 10/11/2021 |
| 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: 6428 Parent PID: 5464

### General

| | |
|---|---|
| Start time: | 03:46:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 6429 Parent PID: 6428

### General

| | |
|---|---|
| Start time: | 03:46:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 6429 Parent PID: 6428

### General

| | |
|---|---|
| Start time: | 03:46:47 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-run-session PID: 5467 Parent PID: 5463

### General

| | |
|---|---|
| Start time: | 03:46:05 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |

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

## Analysis Process: gnome-session PID: 5467 Parent PID: 5463

### General

| | |
|---|---|
| Start time: | 03:46:05 |
| Start date: | 10/11/2021 |
| 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: 5467 Parent PID: 5463

### General

| | |
|---|---|
| Start time: | 03:46:05 |
| Start date: | 10/11/2021 |
| 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: 5468 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:05 |
| Start date: | 10/11/2021 |
| 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: 5468 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:05 |
| Start date: | 10/11/2021 |
| 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: 5527 Parent PID: 5468

### General

| | |
|---|---|
| Start time: | 03:46:13 |
| Start date: | 10/11/2021 |
| 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: 5527 Parent PID: 5468

### General

| | |
|---|---|
| Start time: | 03:46:13 |
| Start date: | 10/11/2021 |
| 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: 5536 Parent PID: 5468

### General

| | |
|---|---|
| Start time: | 03:46:14 |
| Start date: | 10/11/2021 |
| 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: 5536 Parent PID: 5468

### General

| | |
|---|---|
| Start time: | 03:46:14 |
| Start date: | 10/11/2021 |
| 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: 5565 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:17 |
| Start date: | 10/11/2021 |
| 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: 5565 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:17 |
| Start date: | 10/11/2021 |
| 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: 5566 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:17 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

##### Directory Enumerated

## Analysis Process: sh PID: 5566 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:17 |
| Start date: | 10/11/2021 |
| 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: 5566 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:17 |
| Start date: | 10/11/2021 |
| 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: 5566

### General

| | |
|---|---|
| Start time: | 03:46:28 |
| Start date: | 10/11/2021 |
| 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: 5566

### General

| | |
|---|---|
| Start time: | 03:46:28 |
| Start date: | 10/11/2021 |
| 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: 5864 Parent PID: 5623

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

### File Activities

Directory Enumerated

## Analysis Process: ibus-memconf PID: 5864 Parent PID: 5623

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| 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: 5866 Parent PID: 5623

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

## Analysis Process: ibus-daemon PID: 5867 Parent PID: 5866

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

### File Activities

Directory Enumerated

## Analysis Process: ibus-x11 PID: 5867 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:29 |
| Start date: | 10/11/2021 |
| 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: 6133 Parent PID: 5623

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| 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: 6133 Parent PID: 5623

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| 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: 6110 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6110 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| 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: 6110 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| 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: 6112 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6112 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| 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: 6112 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| 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: 6114 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6114 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| 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 |

#### File Activities

#### File Read

## Analysis Process: gsd-color PID: 6114 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-color |
| Arguments: | /usr/libexec/gsd-color |
| File size: | 92832 bytes |
| MD5 hash: | ac2861ad93ce047283e8e87cefef9a19 |

#### File Activities

#### File Read

#### File Written

#### Directory Enumerated

#### Directory Created

## Analysis Process: gnome-session-binary PID: 6115 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6115 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:37 |
| Start date: | 10/11/2021 |
| 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 |

#### File Activities

File Read

## Analysis Process: gsd-keyboard PID: 6115 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-keyboard |
| Arguments: | /usr/libexec/gsd-keyboard |
| File size: | 39760 bytes |
| MD5 hash: | 8e288fd17c80bb0a1148b964b2ac2279 |

### File Activities

File Read

File Written

Directory Enumerated

Directory Created

## Analysis Process: gnome-session-binary PID: 6116 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

Directory Enumerated

## Analysis Process: sh PID: 6116 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| 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 |

### File Activities

File Read

## Analysis Process: gsd-print-notifications PID: 6116 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | /usr/libexec/gsd-print-notifications |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

### File Activities

#### File Read

## Analysis Process: gsd-print-notifications PID: 6150 Parent PID: 6116

### General

| | |
|---|---|
| Start time: | 03:46:45 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | n/a |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

## Analysis Process: gsd-print-notifications PID: 6152 Parent PID: 6150

### General

| | |
|---|---|
| Start time: | 03:46:45 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | n/a |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

### File Activities

#### Directory Enumerated

## Analysis Process: gsd-printer PID: 6152 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:46 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-printer |
| Arguments: | /usr/libexec/gsd-printer |
| File size: | 31120 bytes |
| MD5 hash: | 7995828cf98c315fd55f2ffb3b22384d |

### File Activities

#### File Read

## Analysis Process: gnome-session-binary PID: 6117 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6117 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| 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 |

### File Activities

#### File Read

## Analysis Process: gsd-rfkill PID: 6117 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-rfkill |
| Arguments: | /usr/libexec/gsd-rfkill |
| File size: | 51808 bytes |
| MD5 hash: | 88a16a3c0aba1759358c06215ecfb5cc |

### File Activities

#### File Read

## Analysis Process: gnome-session-binary PID: 6118 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6118 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| 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 |

### File Activities

#### File Read

## Analysis Process: gsd-smartcard PID: 6118 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-smartcard |
| Arguments: | /usr/libexec/gsd-smartcard |
| File size: | 109152 bytes |
| MD5 hash: | ea1fbd7f62e4cd0331eae2ef754ee605 |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated

#### Directory Created

## Analysis Process: gnome-session-binary PID: 6120 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6120 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| 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 |

### File Activities

#### File Read

## Analysis Process: gsd-datetime PID: 6120 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-datetime |
| Arguments: | /usr/libexec/gsd-datetime |
| File size: | 76736 bytes |
| MD5 hash: | d80d39745740de37d6634d36e344d4bc |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated

#### Directory Created

## Analysis Process: gnome-session-binary PID: 6121 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6121 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:39 |
| Start date: | 10/11/2021 |
| 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 |

#### File Activities

##### File Read

## Analysis Process: gsd-media-keys PID: 6121 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-media-keys |
| Arguments: | /usr/libexec/gsd-media-keys |
| File size: | 232936 bytes |
| MD5 hash: | a425448c135afb4b8bfd79cc0b6b74da |

#### File Activities

##### File Read

##### File Written

##### Directory Enumerated

##### Directory Created

## Analysis Process: gnome-session-binary PID: 6126 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

##### Directory Enumerated

## Analysis Process: sh PID: 6126 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:40 |
| Start date: | 10/11/2021 |
| 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 |

#### File Activities

##### File Read

## Analysis Process: gsd-screensaver-proxy PID: 6126 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-screensaver-proxy |
| Arguments: | /usr/libexec/gsd-screensaver-proxy |
| File size: | 27232 bytes |
| MD5 hash: | 77e309450c87dceee43f1a9e50cc0d02 |

#### File Activities

##### File Read

## Analysis Process: gnome-session-binary PID: 6128 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6128 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| 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: 6128 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-sound |
| Arguments: | /usr/libexec/gsd-sound |
| File size: | 31248 bytes |
| MD5 hash: | 4c7d3fb993463337b4a0eb5c80c760ee |

## Analysis Process: gnome-session-binary PID: 6130 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6130 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| 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: 6130 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:42 |
| Start date: | 10/11/2021 |
| 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: 6134 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6134 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:42 |
| Start date: | 10/11/2021 |
| 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: 6134 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:42 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-housekeeping |
| Arguments: | /usr/libexec/gsd-housekeeping |
| File size: | 51840 bytes |
| MD5 hash: | b55f3394a84976ddb92a2915e5d76914 |

## Analysis Process: gnome-session-binary PID: 6137 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:42 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6137 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:42 |
| Start date: | 10/11/2021 |
| 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: 6137 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:46:43 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-power |
| Arguments: | /usr/libexec/gsd-power |
| File size: | 88672 bytes |
| MD5 hash: | 28b8e1b43c3e7f1db6741ea1ecd978b7 |

## Analysis Process: gnome-session-binary PID: 6978 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:47:07 |
| Start date: | 10/11/2021 |

| | |
|---|---|
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6978 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:47:07 |
| Start date: | 10/11/2021 |
| 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: 6978 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:47:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/spice-vdagent |
| Arguments: | /usr/bin/spice-vdagent |
| File size: | 80664 bytes |
| MD5 hash: | 80fb7f613aa78d1b8a229dbcf4577a9d |

## Analysis Process: gnome-session-binary PID: 6981 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:47:08 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6981 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:47:08 |
| Start date: | 10/11/2021 |
| 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: 6981 Parent PID: 5467

### General

| | |
|---|---|
| Start time: | 03:47:09 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/xbrlapi |
| Arguments: | xbrlapi -q |
| File size: | 166384 bytes |
| MD5 hash: | 0cfe25df39d38af32d6265ed947ca5b9 |

## Analysis Process: gdm3 PID: 5412 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5412 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:47 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gdm3 PID: 5413 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5413 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:47 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gdm3 PID: 5421 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:54 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5421 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 03:45:54 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: systemd PID: 5455 Parent PID: 1860

### General

| | |
|---|---|
| Start time: | 03:45:58 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: pulseaudio PID: 5455 Parent PID: 1860

### General

| | |
|---|---|
| Start time: | 03:45:58 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/pulseaudio |
| Arguments: | /usr/bin/pulseaudio --daemonize=no --log-target=journal |
| File size: | 100832 bytes |
| MD5 hash: | 0c3b4c789d8ffb12b25507f27e14c186 |

## Analysis Process: gvfsd-fuse PID: 5471 Parent PID: 2038

### General

| | |
|---|---|
| Start time: | 03:46:08 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gvfsd-fuse |
| Arguments: | n/a |
| File size: | 47632 bytes |
| MD5 hash: | d18fbf1cbf8eb57b17fac48b7b4be933 |

## Analysis Process: fusermount PID: 5471 Parent PID: 2038

### General

| | |
|---|---|
| Start time: | 03:46:08 |
| Start date: | 10/11/2021 |
| Path: | /bin/fusermount |
| Arguments: | fusermount -u -q -z -- /run/user/1000/gvfs |
| File size: | 39144 bytes |
| MD5 hash: | 576a1b135c82bdcbc97a91acea900566 |

## Analysis Process: systemd PID: 5487 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:09 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-user-runtime-dir PID: 5487 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:09 |
| Start date: | 10/11/2021 |
| 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: 5591 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-localed PID: 5591 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:28 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-localed |
| Arguments: | /lib/systemd/systemd-localed |
| File size: | 43232 bytes |
| MD5 hash: | 1244af9646256d49594f2a8203329aa9 |

## Analysis Process: systemd PID: 5879 Parent PID: 1334

### General

| | |
|---|---|
| Start time: | 03:46:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: pulseaudio PID: 5879 Parent PID: 1334

### General

| | |
|---|---|
| Start time: | 03:46:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/pulseaudio |
| Arguments: | /usr/bin/pulseaudio --daemonize=no --log-target=journal |
| File size: | 100832 bytes |
| MD5 hash: | 0c3b4c789d8ffb12b25507f27e14c186 |

## Analysis Process: systemd PID: 5884 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:33 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: geoclue PID: 5884 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:33 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/geoclue |
| Arguments: | /usr/libexec/geoclue |
| File size: | 301544 bytes |
| MD5 hash: | 30ac5455f3c598dde91dc87477fb19f7 |

## Analysis Process: systemd PID: 6155 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:46 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-hostnamed PID: 6155 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:46:46 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-hostnamed |
| Arguments: | /lib/systemd/systemd-hostnamed |
| File size: | 35040 bytes |
| MD5 hash: | 2cc8a5576629a2d5bd98e49a4b8bef65 |

## Analysis Process: systemd PID: 6507 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:47:01 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: fprintd PID: 6507 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:47:01 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/fprintd |
| Arguments: | /usr/libexec/fprintd |
| File size: | 125312 bytes |
| MD5 hash: | b0d8829f05cd028529b84b061b660e84 |

## Analysis Process: systemd PID: 6715 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:47:03 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-localed PID: 6715 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 03:47:03 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-localed |
| Arguments: | /lib/systemd/systemd-localed |
| File size: | 43232 bytes |

| | |
|---|---|
| MD5 hash: | 1244af9646256d49594f2a8203329aa9 |