ID: 519719
Sample Name: arm7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:22:57
Date: 11/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

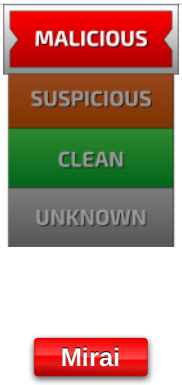
Linux Analysis Report arm7

Overview

General Information

Sample Name:	arm7
Analysis ID:	519719
MD5:	3ac52d54aa5550..
SHA1:	bc1a24e602b2f42.
SHA256:	2a53b47394e367..
Tags:	Mirai
Infos:	

Detection

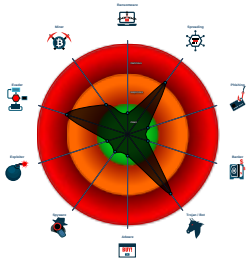


Score:	84
Range:	0 - 100
Whitelisted:	false

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:	519719
Start date:	11.11.2021
Start time:	04:22:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arm7
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@0/51@3/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- arm7 (PID: 5244, Parent: 5118, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm7
  - arm7 New Fork (PID: 5246, Parent: 5244)
  - arm7 New Fork (PID: 5247, Parent: 5244)
    - arm7 New Fork (PID: 5251, Parent: 5247)
    - arm7 New Fork (PID: 5253, Parent: 5247)
      - arm7 New Fork (PID: 5255, Parent: 5253)
- systemd New Fork (PID: 5293, Parent: 1)
- whoopsie (PID: 5293, 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: 5324, Parent: 1320)
  - Default (PID: 5324, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5327, Parent: 1320)
  - Default (PID: 5327, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5328, Parent: 1)
  - accounts-daemon (PID: 5328, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5348, Parent: 5328)
    - language-validate (PID: 5348, Parent: 5328, 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: 5359, Parent: 5353)
    - gdm-wayland-session (PID: 5359, 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: 5362, Parent: 5359)
      - dbus-run-session (PID: 5362, Parent: 5359, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5363, Parent: 5362)
        - dbus-daemon (PID: 5363, Parent: 5362, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
          - dbus-daemon New Fork (PID: 5367, Parent: 5363)
            - 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: 5363)
            - 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: 5363)
            - 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: 5363)
            - 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: 5363)
            - 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: 5363)
            - 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: 5363)
            - dbus-daemon New Fork (PID: 5382, Parent: 5381)
            - false (PID: 5382, Parent: 5381, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-run-session New Fork (PID: 5364, Parent: 5362)
        - gnome-session (PID: 5364, Parent: 5362, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary (PID: 5364, Parent: 5362, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
          - gnome-session-binary New Fork (PID: 5383, Parent: 5364)
          - session-migration (PID: 5383, Parent: 5364, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
          - gnome-session-binary New Fork (PID: 5386, Parent: 5364)
          - sh (PID: 5386, Parent: 5364, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
          - gnome-shell (PID: 5386, Parent: 5364, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5392, Parent: 1320)
  - gdm-session-worker (PID: 5392, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5417, Parent: 5392)
    - gdm-x-session (PID: 5417, Parent: 5392, 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: 5421, Parent: 5417)
      - Xorg (PID: 5421, Parent: 5417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg.wrap (PID: 5421, Parent: 5417, 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: 5421, Parent: 5417, 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: 5433, Parent: 5421)
        - sh (PID: 5433, Parent: 5421, 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: 5434, Parent: 5433)
          - xkbcomp (PID: 5434, Parent: 5433, 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: 5861, Parent: 5421)
        - sh (PID: 5861, Parent: 5421, 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: 5862, Parent: 5861)
          - xkbcomp (PID: 5862, Parent: 5861, 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: 5454, Parent: 5417)
      - Default (PID: 5454, Parent: 5417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
      - gdm-x-session New Fork (PID: 5455, Parent: 5417)
      - dbus-run-session (PID: 5455, Parent: 5417, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart

- dbus-run-session New Fork (PID: 5456, Parent: 5455)
- dbus-daemon (PID: 5456, Parent: 5455, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
  - dbus-daemon New Fork (PID: 5473, Parent: 5456)
    - dbus-daemon New Fork (PID: 5474, Parent: 5473)
    - at-spi-bus-launcher (PID: 5474, Parent: 5473, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
      - at-spi-bus-launcher New Fork (PID: 5510, Parent: 5474)
      - dbus-daemon (PID: 5510, Parent: 5474, 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: 6090, Parent: 5510)
          - dbus-daemon New Fork (PID: 6091, Parent: 6090)
          - at-spi2-registryd (PID: 6091, Parent: 6090, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
  - dbus-daemon New Fork (PID: 5539, Parent: 5456)
    - dbus-daemon New Fork (PID: 5540, Parent: 5539)
    - false (PID: 5540, Parent: 5539, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5542, Parent: 5456)
    - dbus-daemon New Fork (PID: 5543, Parent: 5542)
    - false (PID: 5543, Parent: 5542, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5544, Parent: 5456)
    - dbus-daemon New Fork (PID: 5545, Parent: 5544)
    - false (PID: 5545, Parent: 5544, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5546, Parent: 5456)
    - dbus-daemon New Fork (PID: 5547, Parent: 5546)
    - false (PID: 5547, Parent: 5546, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5548, Parent: 5456)
    - dbus-daemon New Fork (PID: 5549, Parent: 5548)
    - false (PID: 5549, Parent: 5548, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5550, Parent: 5456)
    - dbus-daemon New Fork (PID: 5551, Parent: 5550)
    - false (PID: 5551, Parent: 5550, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5553, Parent: 5456)
    - dbus-daemon New Fork (PID: 5554, Parent: 5553)
    - false (PID: 5554, Parent: 5553, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-daemon New Fork (PID: 5859, Parent: 5456)
    - dbus-daemon New Fork (PID: 5860, Parent: 5859)
    - ibus-portal (PID: 5860, Parent: 5859, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
  - dbus-daemon New Fork (PID: 6094, Parent: 5456)
    - dbus-daemon New Fork (PID: 6095, Parent: 6094)
    - gjs (PID: 6095, Parent: 6094, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
  - dbus-daemon New Fork (PID: 6433, Parent: 5456)
    - dbus-daemon New Fork (PID: 6434, Parent: 6433)
    - false (PID: 6434, Parent: 6433, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-run-session New Fork (PID: 5457, Parent: 5455)
- gnome-session (PID: 5457, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
- gnome-session-binary (PID: 5457, Parent: 5455, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
  - gnome-session-binary New Fork (PID: 5458, Parent: 5457)
  - gnome-session-check-accelerated (PID: 5458, Parent: 5457, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
    - gnome-session-check-accelerated New Fork (PID: 5511, Parent: 5458)
    - gnome-session-check-accelerated-gl-helper (PID: 5511, Parent: 5458, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
    - gnome-session-check-accelerated New Fork (PID: 5528, Parent: 5458)
    - gnome-session-check-accelerated-gles-helper (PID: 5528, Parent: 5458, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
  - gnome-session-binary New Fork (PID: 5557, Parent: 5457)
  - session-migration (PID: 5557, Parent: 5457, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
  - gnome-session-binary New Fork (PID: 5558, Parent: 5457)
  - sh (PID: 5558, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
  - gnome-shell (PID: 5558, Parent: 5457, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
    - gnome-shell New Fork (PID: 5736, Parent: 5558)
    - ibus-daemon (PID: 5736, Parent: 5558, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
      - ibus-daemon New Fork (PID: 5855, Parent: 5736)
      - ibus-memconf (PID: 5855, Parent: 5736, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
      - ibus-daemon New Fork (PID: 5857, Parent: 5736)
        - ibus-daemon New Fork (PID: 5858, Parent: 5857)
        - ibus-x11 (PID: 5858, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
      - ibus-daemon New Fork (PID: 6127, Parent: 5736)
      - ibus-engine-simple (PID: 6127, Parent: 5736, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
  - gnome-session-binary New Fork (PID: 6114, Parent: 5457)
  - sh (PID: 6114, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
  - gsd-sharing (PID: 6114, Parent: 5457, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
  - gnome-session-binary New Fork (PID: 6116, Parent: 5457)
  - sh (PID: 6116, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
  - gsd-wacom (PID: 6116, Parent: 5457, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
  - gnome-session-binary New Fork (PID: 6118, Parent: 5457)
  - sh (PID: 6118, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
  - gsd-color (PID: 6118, Parent: 5457, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
  - gnome-session-binary New Fork (PID: 6119, Parent: 5457)
  - sh (PID: 6119, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
  - gsd-keyboard (PID: 6119, Parent: 5457, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
  - gnome-session-binary New Fork (PID: 6121, Parent: 5457)
  - sh (PID: 6121, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6121, Parent: 5457, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6159, Parent: 6121)

- gsd-print-notifications New Fork (PID: 6220, Parent: 6159)
- gsd-printer (PID: 6220, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 6124, Parent: 5457)
- sh (PID: 6124, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
- gsd-rfkill (PID: 6124, Parent: 5457, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6126, Parent: 5457)
- sh (PID: 6126, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
- gsd-smartcard (PID: 6126, Parent: 5457, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6128, Parent: 5457)
- sh (PID: 6128, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
- gsd-datetime (PID: 6128, Parent: 5457, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6131, Parent: 5457)
- sh (PID: 6131, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
- gsd-media-keys (PID: 6131, Parent: 5457, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6133, Parent: 5457)
- sh (PID: 6133, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
- gsd-screensaver-proxy (PID: 6133, Parent: 5457, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6135, Parent: 5457)
- sh (PID: 6135, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
- gsd-sound (PID: 6135, Parent: 5457, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6138, Parent: 5457)
- sh (PID: 6138, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
- gsd-a11y-settings (PID: 6138, Parent: 5457, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6141, Parent: 5457)
- sh (PID: 6141, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 6141, Parent: 5457, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6144, Parent: 5457)
- sh (PID: 6144, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
- gsd-power (PID: 6144, Parent: 5457, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6986, Parent: 5457)
- sh (PID: 6986, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
- spice-vdagent (PID: 6986, Parent: 5457, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 6992, Parent: 5457)
- sh (PID: 6992, Parent: 5457, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
- xbrlapi (PID: 6992, Parent: 5457, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q

- gdm3 New Fork (PID: 5393, Parent: 1320)
- Default (PID: 5393, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5414, Parent: 1320)
- Default (PID: 5414, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5424, Parent: 1320)
- Default (PID: 5424, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5437, Parent: 1860)
- pulseaudio (PID: 5437, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gvfsd-fuse New Fork (PID: 5476, Parent: 2038)
- fusermount (PID: 5476, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5496, Parent: 1)
- systemd-user-runtime-dir (PID: 5496, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5583, Parent: 1)
- systemd-localed (PID: 5583, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5870, Parent: 1334)
- pulseaudio (PID: 5870, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5873, Parent: 1)
- geoclue (PID: 5873, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6161, Parent: 1)
- systemd-hostnamed (PID: 6161, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6492, Parent: 1)
- systemd-localed (PID: 6492, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 6774, Parent: 1)
- fprintd (PID: 6774, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
arm7	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xafbc:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xb02b:$s2: $Id: UPX • 0xafdc:$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

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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

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

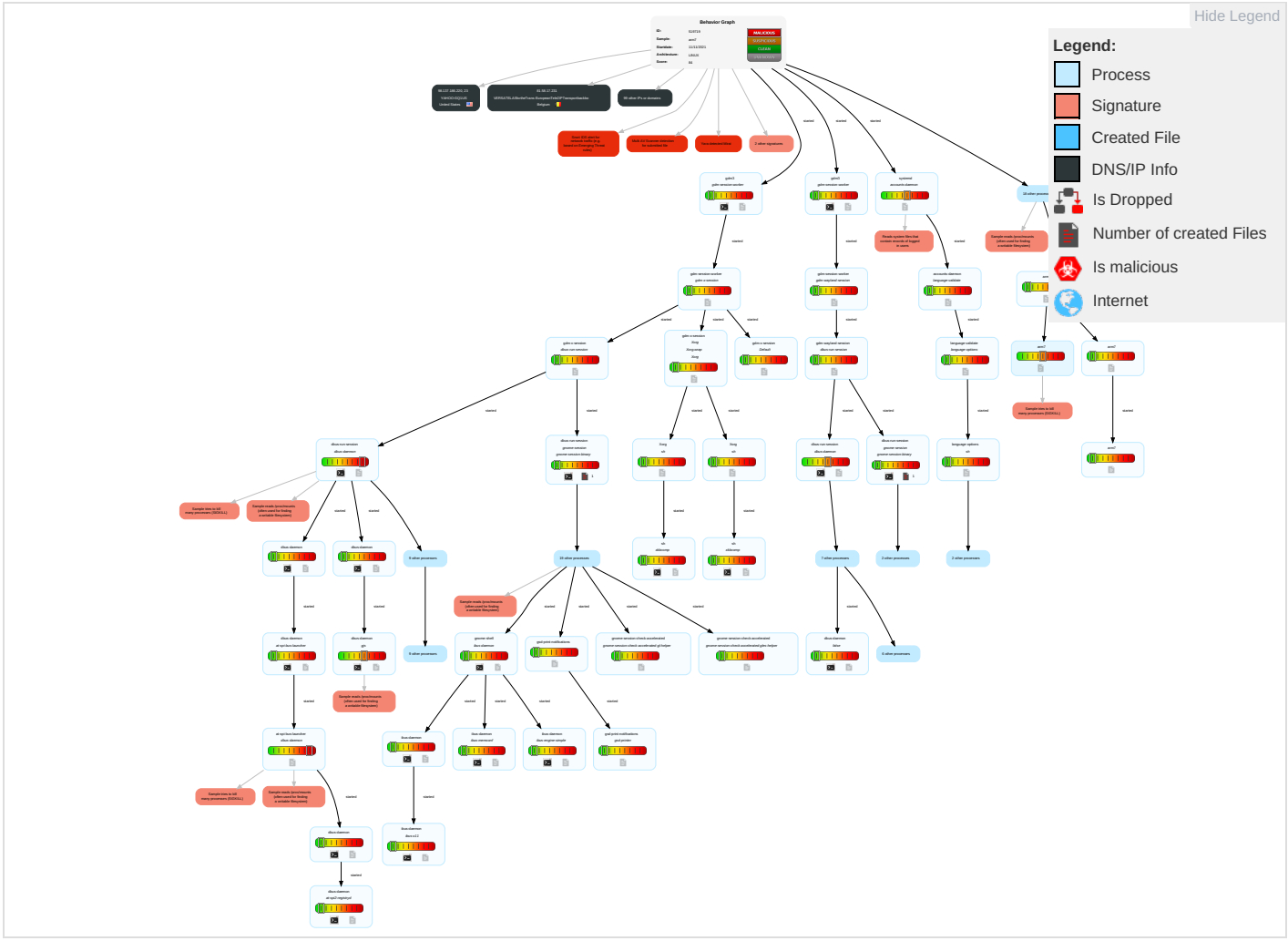
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	Modify System Partitio
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	Device Lockou
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	Delete Device Data
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		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Indicator Removal on Host 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipu App St Rankin or Ratir

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arm7	18%	Virustotal		Browse
arm7	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
102.233.125.222	unknown	unknown		36926	CKL1-ASNKE	false
78.218.236.140	unknown	France		12322	PROXADFR	false
181.18.62.83	unknown	Venezuela		27889	TelecomunicacionesMOVILNETVE	false
172.152.49.110	unknown	United States		7018	ATT-INTERNET4US	false
92.83.24.178	unknown	Romania		9050	RTDBucharestRomaniaRO	false
39.64.200.116	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
4.81.153.118	unknown	United States		3356	LEVEL3US	false
19.108.160.107	unknown	United States		3	MIT-GATEWAYSUS	false
124.229.96.184	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
87.74.162.63	unknown	United Kingdom		25310	ASN-CWACCESSGB	false
57.252.125.35	unknown	Belgium		2686	ATGS-MMD-ASUS	false
60.137.207.70	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
196.86.186.135	unknown	Morocco		6713	IAM-ASMA	false
208.93.2.243	unknown	United States		20419	NETBLK-DMRCOMUS	false
118.181.224.157	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
125.150.108.30	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
41.183.96.133	unknown	South Africa		37028	FNBCONNECTZA	false
172.195.226.39	unknown	Australia		18747	IFX18747US	false
97.21.13.245	unknown	United States		22394	CELLCOUS	false
84.95.60.115	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	false
124.248.198.79	unknown	Hong Kong		4646	SUNNYVISIONSunnyVisionLimitedHK	false
118.85.231.198	unknown	China		4809	CHINATELECOM-CORE-WAN-CN2ChinaTelecomNextGenerationCarr	false
5.130.60.48	unknown	Russian Federation		31200	NTKIPv6customersRU	false
88.46.176.34	unknown	Italy		3269	ASN-IBSNAZIT	false
91.130.14.14	unknown	Austria		1257	TELE2EU	false
112.0.135.246	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
91.52.65.166	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
132.246.240.173	unknown	Canada		25689	SSC-299-25689CA	false
100.57.32.230	unknown	United States		701	UUNETUS	false
211.41.216.119	unknown	Korea Republic of		9943	KNCTV-ASKangNamCableTVKR	false
161.58.239.216	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
178.211.49.197	unknown	Turkey		42926	RADORETR	false
114.201.2.14	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
57.213.33.248	unknown	Belgium		2686	ATGS-MMD-ASUS	false
126.85.3.177	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
76.226.164.60	unknown	United States		7018	ATT-INTERNET4US	false
126.3.138.66	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
177.72.20.48	unknown	Brazil		262691	CONECTALTDABR	false
114.165.235.177	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
70.108.52.29	unknown	United States		701	UUNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
60.141.152.168	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
12.125.15.35	unknown	United States		7018	ATT-INTERNET4US	false
118.128.100.237	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
143.152.230.1	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
31.64.109.81	unknown	United Kingdom		12576	EELtdGB	false
42.3.185.111	unknown	Hong Kong		4760	HKTIMS-APHKTLimitedHK	false
89.187.44.123	unknown	Moldova Republic of		25129	MONITORING-ASMD	false
135.232.5.21	unknown	United States		10455	LUCENT-CIOUS	false
154.10.35.122	unknown	Korea Republic of		9578	CJNET-ASCheiljedangCoIncKR	false
128.227.72.73	unknown	United States		6356	NERDCNETUS	false
117.47.253.132	unknown	Thailand		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
76.201.244.112	unknown	United States		7018	ATT-INTERNET4US	false
36.158.136.114	unknown	China		56047	CMNET-HUNAN-APChinaMobilecommunicationscorporationCN	false
117.106.133.114	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
53.113.156.205	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
80.48.28.80	unknown	Poland		5617	TPNETPL	false
163.175.224.201	unknown	Netherlands		57506	ASN-PDMTNO	false
179.172.101.86	unknown	Brazil		26599	TELEFONICABRASILSABR	false
81.58.17.231	unknown	Belgium		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
2.126.221.17	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
151.30.126.81	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
197.75.183.150	unknown	South Africa		16637	MTNNS-ASZA	false
188.125.174.125	unknown	Turkey		49632	DATATELEKOMTR	false
111.240.86.162	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
70.98.251.121	unknown	United States		10587	FIBERPIPEUS	false
178.198.202.29	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
119.145.130.27	unknown	China		134764	CT-FOSHAN-IDCCHINANETGuangdongprovincenetworkCN	false
218.48.113.16	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
197.73.132.129	unknown	South Africa		16637	MTNNS-ASZA	false
160.13.162.120	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
130.254.133.105	unknown	United States		18759	SAV-ASUS	false
32.17.114.188	unknown	United States		2686	ATGS-MMD-ASUS	false
43.160.107.77	unknown	Japan		4249	LILLY-ASUS	false
148.76.99.191	unknown	United States		6128	CABLE-NET-1US	false
95.194.237.230	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
39.32.71.178	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
46.198.63.212	unknown	Cyprus		6866	CYTA-NETWORKInternetServicesCY	false
17.139.169.80	unknown	United States		714	APPLE-ENGINEERINGUS	false
71.137.108.224	unknown	United States		7018	ATT-INTERNET4US	false
200.193.105.69	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
195.126.43.153	unknown	Germany		702	UUNETUS	false
189.86.165.237	unknown	Brazil		4230	CLAROSABR	false
39.126.211.63	unknown	Korea Republic of		7562	HCNSEOCHO-AS-KRHCNDongjakKR	false
13.103.83.161	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
175.152.229.198	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
178.17.68.63	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
185.226.106.152	unknown	Spain		207046	REDSERVICIOES	false
46.92.247.163	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
199.255.120.35	unknown	United States		40627	RC-COLO1US	false
2.91.119.2	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
148.119.111.121	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
204.211.64.111	unknown	United States		6559	NCIHUS	false
181.201.185.172	unknown	Chile		7418	TELEFONICACHILESACL	false
41.121.55.44	unknown	South Africa		16637	MTNNS-ASZA	false
48.160.163.212	unknown	United States		2686	ATGS-MMD-ASUS	false
189.3.115.151	unknown	Brazil		4230	CLAROSABR	false
161.106.193.148	unknown	France		2278	ORANGELABSOrangeLabsOLPSEU	false
66.191.240.163	unknown	United States		20115	CHARTER-20115US	false
98.137.186.220	unknown	United States		36647	YAHOO-GQ1US	false
179.205.121.74	unknown	Brazil		26615	TIMSABR	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
178.211.49.197	vz3I1CuJPQ	Get hash	malicious	Browse	
91.52.65.166	BitmCvTrdO	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.132
	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.108
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TelecomunicacionesMOVILNETVE	x86_64	Get hash	malicious	Browse	• 181.35.94.106
	dYgJ72oG4f	Get hash	malicious	Browse	• 181.17.48.151
	lYmYPlzghQ	Get hash	malicious	Browse	• 181.17.48.157
	arm7	Get hash	malicious	Browse	• 181.17.223.27

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	wRmHCEnowl	Get hash	malicious	Browse	• 181.17.48.154
	5BfhgIXvAy	Get hash	malicious	Browse	• 181.18.62.52
	SecuriteInfo.com.Linux.Mirai.1429.15365.3177	Get hash	malicious	Browse	• 181.18.62.54
	R9kV5GcwPz	Get hash	malicious	Browse	• 181.17.147.100
	DPJPYxGxfI	Get hash	malicious	Browse	• 181.18.37.41
	g22kPe2LIc	Get hash	malicious	Browse	• 181.18.62.60
	b3astmode.arm	Get hash	malicious	Browse	• 181.35.46.235
	8g3tc5SWwB	Get hash	malicious	Browse	• 181.17.147.111
	5VgU7cIQmK	Get hash	malicious	Browse	• 181.17.147.125
	666.arm7	Get hash	malicious	Browse	• 181.19.238.201
	SYyxBAju45	Get hash	malicious	Browse	• 181.19.238.215
	5NKkJ6URW0	Get hash	malicious	Browse	• 181.17.223.22
	b3astmode.arm	Get hash	malicious	Browse	• 181.35.7.3
	mFKC2tSCJX	Get hash	malicious	Browse	• 181.34.254.116
	b3astmode.x86-20211011-1850	Get hash	malicious	Browse	• 181.19.236.90
	ntpclient	Get hash	malicious	Browse	• 181.18.0.84
CKL1-ASNKE	mF0Mqdkjfz	Get hash	malicious	Browse	• 102.195.48.38
	sora.mips	Get hash	malicious	Browse	• 154.154.144.106
	s36oh8l6l0	Get hash	malicious	Browse	• 102.196.108.94
	trynagetmybinsufucker98575.arm7	Get hash	malicious	Browse	• 154.156.195.131
	Yoshi.arm7-20211110-0350	Get hash	malicious	Browse	• 102.194.241.208
	Yoshi.x86-20211110-0350	Get hash	malicious	Browse	• 102.2.61.4
	sora.arm	Get hash	malicious	Browse	• 102.217.46.201
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 154.159.3.7
	mips	Get hash	malicious	Browse	• 102.4.9.25
	qgxgn5fQU1	Get hash	malicious	Browse	• 102.238.238.5
	GB0O1NUtmJ	Get hash	malicious	Browse	• 102.209.153.234
	byxEpar5Zm	Get hash	malicious	Browse	• 102.241.140.246
	kkr4DrMz5L	Get hash	malicious	Browse	• 102.236.129.90
	62G7F4Mgt0	Get hash	malicious	Browse	• 102.242.129.241
	R7PQ7Hmwq8	Get hash	malicious	Browse	• 102.194.241.203
	wuyZAnkXB9	Get hash	malicious	Browse	• 102.203.57.206
	QISwaj96QZ	Get hash	malicious	Browse	• 102.5.127.220
	bZ3EzTJKiD	Get hash	malicious	Browse	• 102.220.88.189
	v7Tqrjux9I	Get hash	malicious	Browse	• 154.154.7.241
	sora.arm	Get hash	malicious	Browse	• 105.230.56.170
PROXADFR	z0x3n.x86-20211110-2150	Get hash	malicious	Browse	• 78.244.4.30
	sora.arm7	Get hash	malicious	Browse	• 88.169.195.134
	z0x3n.arm-20211110-2150	Get hash	malicious	Browse	• 88.176.250.4
	Recharge150x3-uploadgpj.gpj..exe	Get hash	malicious	Browse	• 83.159.194.96
	QXFOZ3Cshc	Get hash	malicious	Browse	• 82.65.147.204
	lDawzTbABc	Get hash	malicious	Browse	• 78.227.140.91
	eGH4d5FDoU	Get hash	malicious	Browse	• 82.67.203.184
	Yoshi.x86-20211110-0350	Get hash	malicious	Browse	• 78.200.7.192
	zD1jpTbFQq	Get hash	malicious	Browse	• 88.189.112.244
	fNrSUTMJ8O	Get hash	malicious	Browse	• 83.157.120.104
	2tdWqgPQPc	Get hash	malicious	Browse	• 91.167.86.199
	8wdtrqd3z0	Get hash	malicious	Browse	• 91.163.170.206
	x86-20211110-0150	Get hash	malicious	Browse	• 91.163.145.21
	sora.x86	Get hash	malicious	Browse	• 88.190.10.49
	x86	Get hash	malicious	Browse	• 78.212.162.138
	fZ9Y8XVXDH	Get hash	malicious	Browse	• 78.211.212.24
	QaCRsRGMyb	Get hash	malicious	Browse	• 91.163.145.53
	QSjpGBd7Gv	Get hash	malicious	Browse	• 91.169.219.64
	fbXTgwatuJ	Get hash	malicious	Browse	• 91.169.219.34
	mips	Get hash	malicious	Browse	• 88.174.249.35

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
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 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 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 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
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99

/proc/5373/oom_score_adj	
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
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA

/proc/5382/oom_score_adj	
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5474/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5540/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5543/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5545/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V

/proc/5545/oom_score_adj	
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5547/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5549/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5551/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5554/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

/proc/5554/oom_score_adj	
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5860/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/6091/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/6095/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/6434/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/6434/oom_score_adj	
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 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:	 5317.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:EF:EF
MD5:	63883F6ED7AEC27C7A8F3582E33DE117
SHA1:	30C48B516C7B1CCE1BE137AF0E429A5E3B52A645
SHA-256:	4763150DA21E6EED9EDF287DC4B99DCAA83C53510D3ACC76B993B08932B1E7B9
SHA-512:	71B9F090DE8F460A407A9D594327B4104C6EE1933EAF84C8BF1AD2A4D1EE98C60FEC6AC4E1311A4D5849F8E4EA18FE3A20343C1AC46DB58477857CF888DC12 F
Malicious:	false
Preview:	 5437.

/run/user/127/ICEauthority	
Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	5.999713966875013
Encrypted:	false
SSDEEP:	12:OxPDCXMkveY+Dil2xPWVS2xRveY+WU/xP5mhijveY+5tWmxPwWoveY+wcZVveY+B:jJHS2mwqrxwmYwAg
MD5:	193B96241DFAC0CAFE5289C44B6D51F1
SHA1:	76D24499816DD12A7EC4BB8845DF1EED23EACFCE
SHA-256:	1181A7908D420333A2D08257202625D02CAC246F55531A63394D22ECB47751E0
SHA-512:	47F202B97F3684D2E6BA89FF3A780FA1FB40D9B38700ADF041821EDA8978A9578EF27C0516E2E8CC45F4A462A621C634B9D78EFB6D849EA5453AC71CAD58F45
Malicious:	false
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5457..MIT-MAGIC-COOKIE-1.. v.<.W..H.:.".O...XSMP...#local/galassia:@/tmp/.ICE-unix/5457..MIT-MAGIC-COOKIE-1... ..`....G&N ....ICE...!unix/galassia:/tmp/.ICE-unix/5364..MIT-MAGIC-COOKIE-1....I....S....E.Q..ICE...#local/galassia:@/tmp/.ICE-unix/5364..MIT-MAGIC-COOKIE-1..F.#.d/ ./>.Te .}..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

/run/user/127/dconf/user	
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):	4.8653653400210795
Encrypted:	false
SSDEEP:	3:rg/WFllasO93FzHWFllasO93F3:rg/WFl2VDWFl2V3
MD5:	A08B6F53539A6267E8D5238823FEEBED
SHA1:	7335AB1348D6976A4E4FFC3D1B34B4E207645C3B
SHA-256:	EE9CE52BC989F64FCA9C4C4766C9D8577CC9D09DF29F88373F0A91A92FCB37AC
SHA-512:	53C4B1AD3A2A8CD9EB83484CF4C8119AFBA9540E60E87AC8E9BE2075E2DB99A46D4BFCB0B219A8325B9FC766675A89385243ED18B52A2B78AD2527DA6500F8F
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1...X. ...]>gvO.6T....galassia....MIT-MAGIC-COOKIE-1...X. ...]>gvO.6T

/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:Imv:IY
MD5:	2EFD183BB3613F61BFE201210AD7B770
SHA1:	7DE336CBB23FC55CD74D8AE8F24AAA956CB6B741
SHA-256:	87BAEE03B7CB5C0123998D60AFE6169E2887C6039FA13DE276412340B43E6748
SHA-512:	A401CDFAA882359BCFBD2F13C39043366AF4F12E366C3DAD197B3E0DAD1C1D1E95079229265C5E6F2EC7A518BC5A3265F47292C930AB98F2E942C9D0230DC1D
Malicious:	false
Preview:	5870.

/tmp/server-0.xkm	
Process:	/usr/bin/xkbcomp
File Type:	Compiled XKB Keymap: lsb, version 15
Category:	dropped
Size (bytes):	12060
Entropy (8bit):	4.8492493153178975
Encrypted:	false
SSDEEP:	192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ
MD5:	B4E3EB0B8B6B0FC1F46740C573E18D86
SHA1:	7D35426357695EBA77850757E8939A62DCEFF2D1
SHA-256:	7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91
SHA-512:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE01
Malicious:	false

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

/var/lib/AccountsService/users/gdm.9M46B1	
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 AEA
Malicious:	false
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/AccountsService/users/gdm.L5X6B1	
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 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
File Type:	ASCII text
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.176230767677719
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWAhFdq5719W:q5sU3LWfLUDmQymqSFbfomSEg57fW
MD5:	896E3BF9ACDB896DF930102F76C10C5A
SHA1:	C7018BD0E86DCC1DBA5E78F3D76B90846832C056
SHA-256:	0E4354A7770E3D632847765D32DDC00BDA08FA2921D968FEB282B4B2BF22F267
SHA-512:	03205DC4BDDF2405ADECB701D96C0483AED4005035EC86A5477921378FDF7B477458296692F5A38C026FD575FB5DF740A085FF9ED321F2A58623B94E70D02BBE
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-upIQODLF,guid=f60 882bb5f5622c8277d4ec4618c9b39.IBUS_DAEMON_PID=5736.

/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

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE(9
Malicious:	false
Preview:	.

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

/var/lib/whoopsie/whoopsie-id.FINAC1	
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):	5.287748169225308
Encrypted:	false
SSDEEP:	384:E7zxuQaUogMCdhdRd1dJdFdPdmdMdbdZdtdEdid8didedVdKdidcdeTd/JdqVdro:8zxuTbpit7tkBI4WVD/EaO
MD5:	862924DE94D6832285BB9F5759E2AEB9
SHA1:	74EDDAC63E786EEFE7D97F60DFD5D50BE8D2ADD0
SHA-256:	4FC0EEAA67578ACA019E1FDC077B5B0AACB526A00504F58C584B1589F169E9A4
SHA-512:	EA358A5407AB336E9B4D94DDF15AF8A601BAD095B5BF137D47ECB474D0F4A132CE82837F3F3D616222B95C0BD836D6F95BB7B53E79B240A27AF5D2D9B4FD41 C
Malicious:	false
Preview:	[479.915] (--) Log file renamed from "/var/log/Xorg.pid-5421.log" to "/var/log/Xorg.0.log".[479.928] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[4 79.934] Build Operating System: linux Ubuntu.[479.938] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[479.943] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[479.9 53] Build Date: 06 July 2021 10:17:51AM.[479.957] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[479.961] Current version of pixman: 0.38.4.[479.967] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[479.973] 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, EABI4 version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.985627004831107
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm7
File size:	64544
MD5:	3ac52d54aa555033f5095b063a2ea628
SHA1:	bc1a24e602b2f4201bbfaec9f7e0495bdeddb45f
SHA256:	2a53b47394e367a0d4285aa9609938380cf048acbd57d8a18bfb218a0e34c566
SHA512:	d27904d81cd1a94173db1800000ad2ca37e40d09809fd469cdd09862a32856908ea8534c4c0eedfa36cb4b2bbee3cec44922151a4089b0c798e3f76e3f21ec52
SSDEEP:	1536:BB/JzJMY5wBolMP2KSNA5H5GT684wYX6agptUTD0nWJEEkfHW7iLVayMQtJ8hBjn:jcMTKSusiwy6tGBJELf27iL3Oh9
File Content Preview:	.ELF.....(.....$..4.....4. ...(.....x...x...x.....Q.td.....aUPX!.....l.....?.E.h;...#..$...o.....b..~B.*...5N&"a....#R.a..a..,..C....g...k.'..

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:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x124c8
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0xb6b5	0xb6b5	4.0249	0x5	R E	0x8000		
LOAD	0x878	0x30878	0x30878	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 11, 2021 04:24:24.195579052 CET	192.168.2.23	1.1.1.1	0x408e	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Nov 11, 2021 04:24:24.195800066 CET	192.168.2.23	1.1.1.1	0x3e7f	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 11, 2021 04:24:24.315257072 CET	192.168.2.23	1.1.1.1	0xa0f9	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 11, 2021 04:24:24.213287115 CET	1.1.1.1	192.168.2.23	0x408e	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Nov 11, 2021 04:24:24.213287115 CET	1.1.1.1	192.168.2.23	0x408e	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: arm7 PID: 5244 Parent PID: 5118

General

Start time:	04:23:39
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	/tmp/arm7
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: arm7 PID: 5246 Parent PID: 5244

General

Start time:	04:23:39
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5247 Parent PID: 5244

General

Start time:	04:23:39
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5251 Parent PID: 5247

General

Start time:	04:23:39
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5253 Parent PID: 5247

General

Start time:	04:23:39
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5255 Parent PID: 5253

General

Start time:	04:23:39
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5293 Parent PID: 1

General

Start time:	04:24:22
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5293 Parent PID: 1

General

Start time:	04:24:22
Start date:	11/11/2021

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:	04:24:27
Start date:	11/11/2021
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:	04:24:27
Start date:	11/11/2021
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:	04:24:27
Start date:	11/11/2021
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:	04:24:27
Start date:	11/11/2021
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: 5324 Parent PID: 1320

General

Start time:	04:24:34
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5324 Parent PID: 1320

General

Start time:	04:24:34
Start date:	11/11/2021
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: 5327 Parent PID: 1320

General

Start time:	04:24:34
Start date:	11/11/2021
Path:	/usr/sbin/gdm3

Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5327 Parent PID: 1320

General

Start time:	04:24:34
Start date:	11/11/2021
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: 5328 Parent PID: 1

General

Start time:	04:24:34
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5328 Parent PID: 1

General

Start time:	04:24:34
Start date:	11/11/2021
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: 5328

General

Start time:	04:24:34
Start date:	11/11/2021
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: 5328

General

Start time:	04:24:34
Start date:	11/11/2021
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:	04:24:34
Start date:	11/11/2021
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:	04:24:34
Start date:	11/11/2021
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:	04:24:34
Start date:	11/11/2021
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:	04:24:34
Start date:	11/11/2021
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:	04:24:34
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5351 Parent PID: 5350

General

Start time:	04:24:34
Start date:	11/11/2021
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:	04:24:34
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5352 Parent PID: 5350

General

Start time:	04:24:34
Start date:	11/11/2021
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:	04:24:35
Start date:	11/11/2021
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:	04:24:35
Start date:	11/11/2021
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: 5359 Parent PID: 5353

General

Start time:	04:24:37
Start date:	11/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 5359 Parent PID: 5353

General

Start time:	04:24:37
Start date:	11/11/2021
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: 5362 Parent PID: 5359

General

Start time:	04:24:37
Start date:	11/11/2021
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: 5362 Parent PID: 5359

General

Start time:	04:24:37
Start date:	11/11/2021
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: 5363 Parent PID: 5362

General

Start time:	04:24:37
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5363 Parent PID: 5362

General

Start time:	04:24:37
Start date:	11/11/2021
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: 5363

General

Start time:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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: 5363

General

Start time:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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: 5363

General

Start time:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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: 5363

General

Start time:	04:24:39

Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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: 5363

General

Start time:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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: 5363

General

Start time:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021

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: 5363

General

Start time:	04:24:39
Start date:	11/11/2021
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:	04:24:39
Start date:	11/11/2021
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:	04:24:40
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5364 Parent PID: 5362

General

Start time:	04:24:38
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5364 Parent PID: 5362

General

Start time:	04:24:38
Start date:	11/11/2021
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: 5364 Parent PID: 5362

General

Start time:	04:24:38
Start date:	11/11/2021
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: 5364

General

Start time:	04:24:40
Start date:	11/11/2021
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: 5364

General

Start time:	04:24:40
Start date:	11/11/2021
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: 5386 Parent PID: 5364

General

Start time:	04:24:41
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5386 Parent PID: 5364

General

Start time:	04:24:41
Start date:	11/11/2021
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: 5386 Parent PID: 5364

General

Start time:	04:24:41
Start date:	11/11/2021
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: 5392 Parent PID: 1320

General

Start time:	04:24:44
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5392 Parent PID: 1320

General

Start time:	04:24:44
Start date:	11/11/2021
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: 5417 Parent PID: 5392

General

Start time:	04:24:45
Start date:	11/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes

MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 5417 Parent PID: 5392

General

Start time:	04:24:45
Start date:	11/11/2021
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: 5421 Parent PID: 5417

General

Start time:	04:24:46
Start date:	11/11/2021
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: 5421 Parent PID: 5417

General

Start time:	04:24:46
Start date:	11/11/2021
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: 5421 Parent PID: 5417

General

Start time:	04:24:46
Start date:	11/11/2021
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: 5421 Parent PID: 5417

General

Start time:	04:24:46
Start date:	11/11/2021
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: 5433 Parent PID: 5421

General

Start time:	04:24:56
Start date:	11/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5433 Parent PID: 5421

General

Start time:	04:24:56
Start date:	11/11/2021
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: 5434 Parent PID: 5433

General

Start time:	04:24:56
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5434 Parent PID: 5433

General

Start time:	04:24:56
Start date:	11/11/2021
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: 5861 Parent PID: 5421

General

Start time:	04:25:30
Start date:	11/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5861 Parent PID: 5421

General

Start time:	04:25:30
Start date:	11/11/2021

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: 5862 Parent PID: 5861

General

Start time:	04:25:30
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5862 Parent PID: 5861

General

Start time:	04:25:30
Start date:	11/11/2021
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: 5454 Parent PID: 5417

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5454 Parent PID: 5417

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5455 Parent PID: 5417

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5455 Parent PID: 5417

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5456 Parent PID: 5455

General

Start time:	04:25:03
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5456 Parent PID: 5455

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5473 Parent PID: 5456

General

Start time:	04:25:09
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5474 Parent PID: 5473

General

Start time:	04:25:09
Start date:	11/11/2021
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: 5474 Parent PID: 5473

General

Start time:	04:25:09
Start date:	11/11/2021
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: 5510 Parent PID: 5474

General

Start time:	04:25:11
Start date:	11/11/2021
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: 5510 Parent PID: 5474

General

Start time:	04:25:11
Start date:	11/11/2021
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: 6090 Parent PID: 5510

General

Start time:	04:25:33
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 6091 Parent PID: 6090

General

Start time:	04:25:33
Start date:	11/11/2021
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: 6091 Parent PID: 6090

General

Start time:	04:25:33
Start date:	11/11/2021
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: 5539 Parent PID: 5456

General

Start time:	04:25:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5540 Parent PID: 5539

General

Start time:	04:25:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5540 Parent PID: 5539

General

Start time:	04:25:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5542 Parent PID: 5456

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5543 Parent PID: 5542

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5543 Parent PID: 5542

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5544 Parent PID: 5456

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5545 Parent PID: 5544

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5545 Parent PID: 5544

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5546 Parent PID: 5456

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5547 Parent PID: 5546

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5547 Parent PID: 5546

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5548 Parent PID: 5456

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5549 Parent PID: 5548

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5549 Parent PID: 5548

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5550 Parent PID: 5456

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5551 Parent PID: 5550

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5551 Parent PID: 5550

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5553 Parent PID: 5456

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5554 Parent PID: 5553

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5554 Parent PID: 5553

General

Start time:	04:25:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5859 Parent PID: 5456

General

Start time:	04:25:29
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5860 Parent PID: 5859

General

Start time:	04:25:29
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: ibus-portal PID: 5860 Parent PID: 5859

General

Start time:	04:25:29
Start date:	11/11/2021
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: 6094 Parent PID: 5456

General

Start time:	04:25:35
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 6095 Parent PID: 6094

General

Start time:	04:25:35
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: gjs PID: 6095 Parent PID: 6094

General

Start time:	04:25:35
Start date:	11/11/2021
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: 6433 Parent PID: 5456

General

Start time:	04:25:50
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 6434 Parent PID: 6433

General

Start time:	04:25:50
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 6434 Parent PID: 6433

General

Start time:	04:25:51
Start date:	11/11/2021

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

File Activities

File Read

Analysis Process: dbus-run-session PID: 5457 Parent PID: 5455

General

Start time:	04:25:03
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5457 Parent PID: 5455

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5457 Parent PID: 5455

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5458 Parent PID: 5457

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5458 Parent PID: 5457

General

Start time:	04:25:03
Start date:	11/11/2021
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: 5511 Parent PID: 5458

General

Start time:	04:25:12
Start date:	11/11/2021
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: 5511 Parent PID: 5458

General

Start time:	04:25:12
Start date:	11/11/2021
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: 5528 Parent PID: 5458

General

Start time:	04:25:13
Start date:	11/11/2021
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: 5528 Parent PID: 5458

General

Start time:	04:25:13
Start date:	11/11/2021
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: 5557 Parent PID: 5457

General

Start time:	04:25:16

Start date:	11/11/2021
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: 5557 Parent PID: 5457

General

Start time:	04:25:16
Start date:	11/11/2021
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: 5558 Parent PID: 5457

General

Start time:	04:25:17
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5558 Parent PID: 5457

General

Start time:	04:25:17
Start date:	11/11/2021
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: 5558 Parent PID: 5457

General

Start time:	04:25:17
Start date:	11/11/2021
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: 5736 Parent PID: 5558

General

Start time:	04:25:28
Start date:	11/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5736 Parent PID: 5558

General

Start time:	04:25:28
Start date:	11/11/2021
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: 5855 Parent PID: 5736

General

Start time:	04:25:29
Start date:	11/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5855 Parent PID: 5736

General

Start time:	04:25:29
Start date:	11/11/2021
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: 5857 Parent PID: 5736

General

Start time:	04:25:29
Start date:	11/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5858 Parent PID: 5857

General

Start time:	04:25:29

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

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5858 Parent PID: 1

General

Start time:	04:25:29
Start date:	11/11/2021
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: 6127 Parent PID: 5736

General

Start time:	04:25:42
Start date:	11/11/2021
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: 6127 Parent PID: 5736

General

Start time:	04:25:42
Start date:	11/11/2021
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: 6114 Parent PID: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 6114 Parent PID: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 6116 Parent PID: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 6116 Parent PID: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 6118 Parent PID: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 5457

General

Start time:	04:25:39
Start date:	11/11/2021
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: 6118 Parent PID: 5457

General

Start time:	04:25:40
Start date:	11/11/2021
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: 6119 Parent PID: 5457

General

Start time:	04:25:40
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes

MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6119 Parent PID: 5457

General

Start time:	04:25:40
Start date:	11/11/2021
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: 6119 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 6121 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 6121 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 6159 Parent PID: 6121

General

Start time:	04:25:49
Start date:	11/11/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6220 Parent PID: 6159

General

Start time:	04:25:49
Start date:	11/11/2021
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: 6220 Parent PID: 1

General

Start time:	04:25:50
Start date:	11/11/2021
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: 6124 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6124 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 6124 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 6126 Parent PID: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 5457

General

Start time:	04:25:41
Start date:	11/11/2021
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: 6126 Parent PID: 5457

General

Start time:	04:25:42
Start date:	11/11/2021
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: 6128 Parent PID: 5457

General

Start time:	04:25:42
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6128 Parent PID: 5457

General

Start time:	04:25:42
Start date:	11/11/2021
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: 6128 Parent PID: 5457

General

Start time:	04:25:43
Start date:	11/11/2021
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: 6131 Parent PID: 5457

General

Start time:	04:25:43
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6131 Parent PID: 5457

General

Start time:	04:25:43
Start date:	11/11/2021
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: 6131 Parent PID: 5457

General

Start time:	04:25:43
Start date:	11/11/2021
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: 6133 Parent PID: 5457

General

Start time:	04:25:43

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

File Activities

Directory Enumerated

Analysis Process: sh PID: 6133 Parent PID: 5457

General

Start time:	04:25:43
Start date:	11/11/2021
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: 6133 Parent PID: 5457

General

Start time:	04:25:44
Start date:	11/11/2021
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: 6135 Parent PID: 5457

General

Start time:	04:25:43
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6135 Parent PID: 5457

General

Start time:	04:25:44
Start date:	11/11/2021
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

File Activities

File Read

Analysis Process: gsd-sound PID: 6135 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
Path:	/usr/libexec/gsd-sound
Arguments:	/usr/libexec/gsd-sound
File size:	31248 bytes
MD5 hash:	4c7d3fb993463337b4a0eb5c80c760ee

File Activities

File Read

Analysis Process: gnome-session-binary PID: 6138 Parent PID: 5457

General

Start time:	04:25:44
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6138 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
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: 6138 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
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: 6141 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6141 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
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: 6141 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

Analysis Process: gnome-session-binary PID: 6144 Parent PID: 5457

General

Start time:	04:25:45
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6144 Parent PID: 5457

General

Start time:	04:25:46
Start date:	11/11/2021
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: 6144 Parent PID: 5457

General

Start time:	04:25:46
Start date:	11/11/2021
Path:	/usr/libexec/gsd-power
Arguments:	/usr/libexec/gsd-power
File size:	88672 bytes
MD5 hash:	28b8e1b43c3e7f1db6741ea1ecd978b7

Analysis Process: gnome-session-binary PID: 6986 Parent PID: 5457

General

Start time:	04:26:10
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6986 Parent PID: 5457

General

Start time:	04:26:11
Start date:	11/11/2021
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: 6986 Parent PID: 5457

General

Start time:	04:26:11
Start date:	11/11/2021
Path:	/usr/bin/spice-vdagent
Arguments:	/usr/bin/spice-vdagent
File size:	80664 bytes
MD5 hash:	80fb7f613aa78d1b8a229dbcf4577a9d

Analysis Process: gnome-session-binary PID: 6992 Parent PID: 5457

General

Start time:	04:26:12
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6992 Parent PID: 5457

General

Start time:	04:26:12
Start date:	11/11/2021
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: 6992 Parent PID: 5457

General

Start time:	04:26:13
Start date:	11/11/2021
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5393 Parent PID: 1320

General

Start time:	04:24:44
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5393 Parent PID: 1320

General

Start time:	04:24:44
Start date:	11/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5414 Parent PID: 1320

General

Start time:	04:24:44
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5414 Parent PID: 1320

General

Start time:	04:24:44
Start date:	11/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5424 Parent PID: 1320

General

Start time:	04:24:52
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5424 Parent PID: 1320

General

Start time:	04:24:52
Start date:	11/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemd PID: 5437 Parent PID: 1860

General

Start time:	04:24:57
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5437 Parent PID: 1860

General

Start time:	04:24:57
Start date:	11/11/2021
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: 5476 Parent PID: 2038

General

Start time:	04:25:10
Start date:	11/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5476 Parent PID: 2038

General

Start time:	04:25:10
Start date:	11/11/2021
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

Analysis Process: systemd PID: 5496 Parent PID: 1

General

Start time:	04:25:11
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5496 Parent PID: 1

General

Start time:	04:25:11
Start date:	11/11/2021
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: 5583 Parent PID: 1

General

Start time:	04:25:28
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5583 Parent PID: 1

General

Start time:	04:25:28
Start date:	11/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 5870 Parent PID: 1334

General

Start time:	04:25:32
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5870 Parent PID: 1334

General

Start time:	04:25:32
Start date:	11/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5873 Parent PID: 1

General

Start time:	04:25:33

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

Analysis Process: geoclue PID: 5873 Parent PID: 1

General

Start time:	04:25:33
Start date:	11/11/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 6161 Parent PID: 1

General

Start time:	04:25:50
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-hostnamed PID: 6161 Parent PID: 1

General

Start time:	04:25:50
Start date:	11/11/2021
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	35040 bytes
MD5 hash:	2cc8a5576629a2d5bd98e49a4b8bef65

Analysis Process: systemd PID: 6492 Parent PID: 1

General

Start time:	04:26:06
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 6492 Parent PID: 1

General

Start time:	04:26:06
Start date:	11/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 6774 Parent PID: 1

General

Start time:	04:26:07
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6774 Parent PID: 1

General

Start time:	04:26:07
Start date:	11/11/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84