ID: 506685
Sample Name: arm7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:02:02
Date: 21/10/2021
Version: 33.0.0 White Diamond

Table of Contents

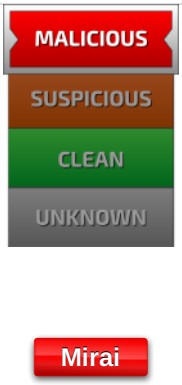
Linux Analysis Report arm7

Overview

General Information

Sample Name:	arm7
Analysis ID:	506685
MD5:	1adc0d120624cd..
SHA1:	5e17dd426d0d53..
SHA256:	3cd04e2c688f17b..
Infos:	

Detection

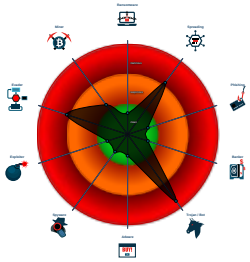


Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

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

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:	33.0.0 White Diamond
Analysis ID:	506685
Start date:	21.10.2021
Start time:	02:02:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
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:	mal96.spre.troj.evad.lin@0/52@3/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- arm7 (PID: 5231, Parent: 5109, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm7
  - arm7 New Fork (PID: 5233, Parent: 5231)
  - arm7 New Fork (PID: 5235, Parent: 5231)
  - arm7 New Fork (PID: 5236, Parent: 5231)
  - arm7 New Fork (PID: 5240, Parent: 5231)
  - arm7 New Fork (PID: 5241, Parent: 5231)
  - arm7 New Fork (PID: 5244, Parent: 5231)
    - arm7 New Fork (PID: 5247, Parent: 5244)

- arm7 New Fork (PID: 5250, Parent: 5244)
  - arm7 New Fork (PID: 5252, Parent: 5250)
- systemd New Fork (PID: 5291, Parent: 1)
- whoopsie (PID: 5291, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5320, Parent: 1)
- sshd (PID: 5320, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5321, Parent: 1)
- sshd (PID: 5321, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- dash New Fork (PID: 5322, Parent: 4333)
- cat (PID: 5322, Parent: 4333, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.ufH0NYtBX2
- dash New Fork (PID: 5323, Parent: 4333)
- head (PID: 5323, Parent: 4333, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5324, Parent: 4333)
- tr (PID: 5324, Parent: 4333, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5325, Parent: 4333)
- cut (PID: 5325, Parent: 4333, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5326, Parent: 4333)
- cat (PID: 5326, Parent: 4333, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.ufH0NYtBX2
- dash New Fork (PID: 5327, Parent: 4333)
- head (PID: 5327, Parent: 4333, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5328, Parent: 4333)
- tr (PID: 5328, Parent: 4333, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5329, Parent: 4333)
- cut (PID: 5329, Parent: 4333, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5330, Parent: 4333)
- rm (PID: 5330, Parent: 4333, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.ufH0NYtBX2 /tmp/tmp.4U2ZRxJPEO /tmp/tmp.Q0Nrki22iD
- gdm3 New Fork (PID: 5337, Parent: 1320)
- Default (PID: 5337, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5340, Parent: 1320)
- Default (PID: 5340, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5341, Parent: 1)
- accounts-daemon (PID: 5341, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5360, Parent: 5341)
  - language-validate (PID: 5360, Parent: 5341, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5361, Parent: 5360)
    - language-options (PID: 5361, Parent: 5360, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5362, Parent: 5361)
      - sh (PID: 5362, Parent: 5361, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5363, Parent: 5362)
        - locale (PID: 5363, Parent: 5362, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5364, Parent: 5362)
        - grep (PID: 5364, Parent: 5362, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm3 New Fork (PID: 5365, Parent: 1320)
- gdm-session-worker (PID: 5365, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5371, Parent: 5365)
  - gdm-wayland-session (PID: 5371, Parent: 5365, 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: 5374, Parent: 5371)
    - dbus-run-session (PID: 5374, Parent: 5371, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
      - dbus-run-session New Fork (PID: 5375, Parent: 5374)
      - dbus-daemon (PID: 5375, Parent: 5374, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5379, Parent: 5375)
          - dbus-daemon New Fork (PID: 5380, Parent: 5379)
          - false (PID: 5380, Parent: 5379, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5382, Parent: 5375)
          - dbus-daemon New Fork (PID: 5383, Parent: 5382)
          - false (PID: 5383, Parent: 5382, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5384, Parent: 5375)
          - dbus-daemon New Fork (PID: 5385, Parent: 5384)
          - false (PID: 5385, Parent: 5384, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5386, Parent: 5375)
          - dbus-daemon New Fork (PID: 5387, Parent: 5386)
          - false (PID: 5387, Parent: 5386, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5388, Parent: 5375)
          - dbus-daemon New Fork (PID: 5389, Parent: 5388)
          - false (PID: 5389, Parent: 5388, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5390, Parent: 5375)
          - dbus-daemon New Fork (PID: 5391, Parent: 5390)
          - false (PID: 5391, Parent: 5390, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5395, Parent: 5375)
          - dbus-daemon New Fork (PID: 5396, Parent: 5395)
          - false (PID: 5396, Parent: 5395, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - dbus-run-session New Fork (PID: 5376, Parent: 5374)
      - gnome-session (PID: 5376, Parent: 5374, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
      - gnome-session-binary (PID: 5376, Parent: 5374, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary New Fork (PID: 5397, Parent: 5376)
        - session-migration (PID: 5397, Parent: 5376, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
        - gnome-session-binary New Fork (PID: 5398, Parent: 5376)
        - sh (PID: 5398, Parent: 5376, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
        - gnome-shell (PID: 5398, Parent: 5376, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5426, Parent: 1320)
- gdm-session-worker (PID: 5426, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5431, Parent: 5426)
  - gdm-x-session (PID: 5431, Parent: 5426, 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: 5435, Parent: 5431)
    - Xorg (PID: 5435, Parent: 5431, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -

noreset -keeptty -verbose 3
- Xorg.wrap (PID: 5435, Parent: 5431, 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: 5435, Parent: 5431, 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: 5476, Parent: 5435)
  - sh (PID: 5476, Parent: 5435, 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: 5477, Parent: 5476)
    - xkbcomp (PID: 5477, Parent: 5476, 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: 5898, Parent: 5435)
  - sh (PID: 5898, Parent: 5435, 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: 5900, Parent: 5898)
    - xkbcomp (PID: 5900, Parent: 5898, 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: 5525, Parent: 5431)
- Default (PID: 5525, Parent: 5431, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
- gdm-x-session New Fork (PID: 5526, Parent: 5431)
- dbus-run-session (PID: 5526, Parent: 5431, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
  - dbus-run-session New Fork (PID: 5527, Parent: 5526)
  - dbus-daemon (PID: 5527, Parent: 5526, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
    - dbus-daemon New Fork (PID: 5543, Parent: 5527)
      - dbus-daemon New Fork (PID: 5544, Parent: 5543)
      - at-spi-bus-launcher (PID: 5544, Parent: 5543, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
        - at-spi-bus-launcher New Fork (PID: 5549, Parent: 5544)
        - dbus-daemon (PID: 5549, Parent: 5544, 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: 5994, Parent: 5549)
            - dbus-daemon New Fork (PID: 5998, Parent: 5994)
            - at-spi2-registryd (PID: 5998, Parent: 5994, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
    - dbus-daemon New Fork (PID: 5573, Parent: 5527)
      - dbus-daemon New Fork (PID: 5574, Parent: 5573)
      - false (PID: 5574, Parent: 5573, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5576, Parent: 5527)
      - dbus-daemon New Fork (PID: 5577, Parent: 5576)
      - false (PID: 5577, Parent: 5576, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5578, Parent: 5527)
      - dbus-daemon New Fork (PID: 5579, Parent: 5578)
      - false (PID: 5579, Parent: 5578, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5580, Parent: 5527)
      - dbus-daemon New Fork (PID: 5581, Parent: 5580)
      - false (PID: 5581, Parent: 5580, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5582, Parent: 5527)
      - dbus-daemon New Fork (PID: 5583, Parent: 5582)
      - false (PID: 5583, Parent: 5582, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5584, Parent: 5527)
      - dbus-daemon New Fork (PID: 5585, Parent: 5584)
      - false (PID: 5585, Parent: 5584, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5587, Parent: 5527)
      - dbus-daemon New Fork (PID: 5588, Parent: 5587)
      - false (PID: 5588, Parent: 5587, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5848, Parent: 5527)
      - dbus-daemon New Fork (PID: 5852, Parent: 5848)
      - ibus-portal (PID: 5852, Parent: 5848, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
    - dbus-daemon New Fork (PID: 6117, Parent: 5527)
      - dbus-daemon New Fork (PID: 6118, Parent: 6117)
      - gjs (PID: 6118, Parent: 6117, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
    - dbus-daemon New Fork (PID: 6180, Parent: 5527)
      - dbus-daemon New Fork (PID: 6181, Parent: 6180)
      - false (PID: 6181, Parent: 6180, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-run-session New Fork (PID: 5528, Parent: 5526)
  - gnome-session (PID: 5528, Parent: 5526, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
  - gnome-session-binary (PID: 5528, Parent: 5526, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
    - gnome-session-binary New Fork (PID: 5529, Parent: 5528)
    - gnome-session-check-accelerated (PID: 5529, Parent: 5528, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
      - gnome-session-check-accelerated New Fork (PID: 5550, Parent: 5529)
      - gnome-session-check-accelerated-gl-helper (PID: 5550, Parent: 5529, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
      - gnome-session-check-accelerated New Fork (PID: 5562, Parent: 5529)
      - gnome-session-check-accelerated-gles-helper (PID: 5562, Parent: 5529, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
    - gnome-session-binary New Fork (PID: 5589, Parent: 5528)
    - session-migration (PID: 5589, Parent: 5528, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
    - gnome-session-binary New Fork (PID: 5590, Parent: 5528)
    - sh (PID: 5590, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
    - gnome-shell (PID: 5590, Parent: 5528, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
      - gnome-shell New Fork (PID: 5648, Parent: 5590)
      - ibus-daemon (PID: 5648, Parent: 5590, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
        - ibus-daemon New Fork (PID: 5782, Parent: 5648)
        - ibus-memconf (PID: 5782, Parent: 5648, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
        - ibus-daemon New Fork (PID: 5814, Parent: 5648)
          - ibus-daemon New Fork (PID: 5818, Parent: 5814)
          - ibus-x11 (PID: 5818, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
        - ibus-daemon New Fork (PID: 6163, Parent: 5648)
        - ibus-engine-simple (PID: 6163, Parent: 5648, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple

- gnome-session-binary New Fork (PID: 6139, Parent: 5528)
  - sh (PID: 6139, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
  - gsd-sharing (PID: 6139, Parent: 5528, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
- gnome-session-binary New Fork (PID: 6141, Parent: 5528)
  - sh (PID: 6141, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
  - gsd-wacom (PID: 6141, Parent: 5528, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 6143, Parent: 5528)
  - sh (PID: 6143, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
  - gsd-color (PID: 6143, Parent: 5528, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 6144, Parent: 5528)
  - sh (PID: 6144, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
  - gsd-keyboard (PID: 6144, Parent: 5528, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 6145, Parent: 5528)
  - sh (PID: 6145, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6145, Parent: 5528, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6191, Parent: 6145)
      - gsd-print-notifications New Fork (PID: 6192, Parent: 6191)
      - gsd-printer (PID: 6192, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 6146, Parent: 5528)
  - sh (PID: 6146, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
  - gsd-rfkill (PID: 6146, Parent: 5528, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6147, Parent: 5528)
  - sh (PID: 6147, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
  - gsd-smartcard (PID: 6147, Parent: 5528, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6149, Parent: 5528)
  - sh (PID: 6149, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
  - gsd-datetime (PID: 6149, Parent: 5528, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6150, Parent: 5528)
  - sh (PID: 6150, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
  - gsd-media-keys (PID: 6150, Parent: 5528, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6151, Parent: 5528)
  - sh (PID: 6151, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
  - gsd-screensaver-proxy (PID: 6151, Parent: 5528, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6154, Parent: 5528)
  - sh (PID: 6154, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
  - gsd-sound (PID: 6154, Parent: 5528, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6156, Parent: 5528)
  - sh (PID: 6156, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
  - gsd-a11y-settings (PID: 6156, Parent: 5528, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6161, Parent: 5528)
  - sh (PID: 6161, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
  - gsd-housekeeping (PID: 6161, Parent: 5528, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6164, Parent: 5528)
  - sh (PID: 6164, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
  - gsd-power (PID: 6164, Parent: 5528, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 7032, Parent: 5528)
  - sh (PID: 7032, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
  - spice-vdagent (PID: 7032, Parent: 5528, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 7039, Parent: 5528)
  - sh (PID: 7039, Parent: 5528, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
  - xbrlapi (PID: 7039, Parent: 5528, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q
- gdm3 New Fork (PID: 5427, Parent: 1320)
  - Default (PID: 5427, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5428, Parent: 1320)
  - Default (PID: 5428, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5436, Parent: 1320)
  - Default (PID: 5436, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5442, Parent: 1860)
  - pulseaudio (PID: 5442, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gvfsd-fuse New Fork (PID: 5482, Parent: 2038)
  - fusermount (PID: 5482, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5500, Parent: 1)
  - systemd-user-runtime-dir (PID: 5500, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5615, Parent: 1)
  - systemd-localed (PID: 5615, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5903, Parent: 1334)
  - pulseaudio (PID: 5903, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5906, Parent: 1)
  - geoclue (PID: 5906, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6193, Parent: 1)
  - systemd-hostnamed (PID: 6193, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6548, Parent: 1)
  - systemd-localed (PID: 6548, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 6813, Parent: 1)

- fprintd (PID: 6813, 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	• 0xc74c:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xc7bb:$s2: $Id: UPX • 0xc76c:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5252.1.000000003b200909.0000000001ef2106.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5235.1.000000003b200909.0000000001ef2106.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5250.1.000000003b200909.0000000001ef2106.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5231.1.000000003b200909.0000000001ef2106.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5236.1.000000003b200909.0000000001ef2106.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 5 entries				

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary:

Sample tries to kill many processes (SIGKILL)

Data Obfuscation:

Sample is packed with UPX

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

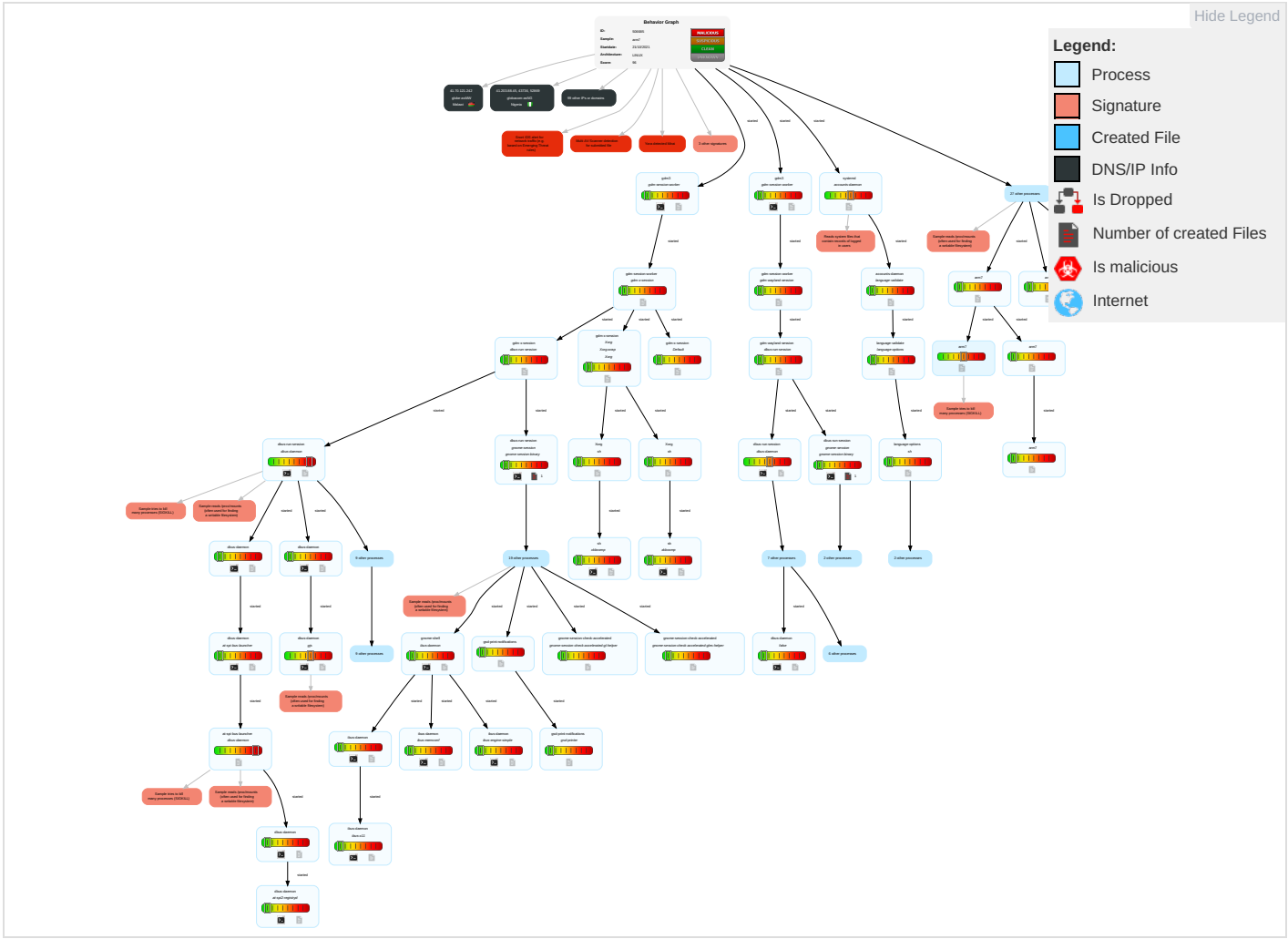
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Valid Accounts	Scripting 1	Path Interception	Path Interception	File and Directory Permissions Modification 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1	LSASS Memory	System Owner/User Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap		C E F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Indicator Removal on Host 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A F F
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		A A F

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arm7	32%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.billybobbot.com/crawler/)	0%	URL Reputation	safe	
http://fast.no/support/crawler.asp)	0%	URL Reputation	safe	
http://23.94.22.102/bins/mips;	0%	Avira URL Cloud	safe	
http://feedback.redkolibri.com/	0%	URL Reputation	safe	

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
37.224.192.125	unknown	Saudi Arabia		39891	ALJAWWALSTC-ASSA	false
41.187.159.158	unknown	Egypt		20928	NOOR-ASEG	false
175.113.154.55	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
113.227.250.126	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
82.222.17.44	unknown	Turkey		34984	TELLCOM-ASTR	false
197.51.4.209	unknown	Egypt		8452	TE-ASTE-ASEG	false
119.235.133.72	unknown	China		24427	CNNIC-FREENETFreecommCorporationCN	false
156.67.35.90	unknown	United Kingdom		48101	CALLFLOW-ASCallFlowSolutionsLtdGB	false
23.245.1.206	unknown	United States		18978	ENZUINC-US	false
189.215.130.156	unknown	Mexico		28538	CablemasTelecomunicacionesSAdeCVMX	false
197.103.64.207	unknown	South Africa		3741	ISZA	false
156.1.114.137	unknown	United States		22226	SFUSDUS	false
63.234.234.120	unknown	United States		12068	RC-ASNUS	false
175.5.191.20	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
197.4.54.12	unknown	Tunisia		5438	ATI-TN	false
116.217.68.0	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
197.58.204.206	unknown	Egypt		8452	TE-ASTE-ASEG	false
144.138.185.204	unknown	Australia		135887	TELSTRA-BELONG-APTelstraCorporationAU	false
41.36.218.213	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.160.244.188	unknown	Egypt		24863	LINKdotNET-ASEG	false
52.255.11.162	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
80.183.157.45	unknown	Italy		3269	ASN-IBSNAZIT	false
86.21.5.214	unknown	United Kingdom		5089	NTLGB	false
41.157.30.86	unknown	South Africa		37168	CELL-CZA	false
41.102.136.80	unknown	Algeria		36947	ALGTEL-ASDZ	false
43.85.133.173	unknown	Japan		4249	LILLY-ASUS	false
17.40.3.210	unknown	United States		714	APPLE-ENGINEERINGUS	false
61.104.167.126	unknown	Korea Republic of		38117	JS89005-AS-KRjinsancablenetcompanyltdKR	false
41.182.10.64	unknown	Namibia		36996	TELECOM-NAMIBIANA	false
197.32.129.161	unknown	Egypt		8452	TE-ASTE-ASEG	false
105.167.236.215	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
41.216.98.146	unknown	Mauritius		37006	LiquidTelecommunicationRwandaRW	false
147.124.88.10	unknown	United States		1432	AC-AS-1US	false
197.213.165.219	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
41.21.227.66	unknown	South Africa		36994	Vodacom-VBZA	false
194.221.100.200	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
41.9.179.0	unknown	South Africa		29975	VODACOM-ZA	false
177.106.15.111	unknown	Brazil		53006	ALGARTELECOMSABR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.11.35.25	unknown	Canada		15290	ALLST-15290CA	false
104.62.108.179	unknown	United States		7018	ATT-INTERNET4US	false
146.10.238.116	unknown	United States		197938	TRAVIANGAMESDE	false
35.221.252.39	unknown	United States		15169	GOOGLEUS	false
197.126.118.198	unknown	Egypt		36992	ETISALAT-MISREG	false
197.20.132.116	unknown	Tunisia		37693	TUNISIANATN	false
121.95.0.18	unknown	Japan		2510	INFOWEBFUJITSULIMITED JP	false
131.135.18.169	unknown	Canada		74	SSC-299-Z-74CA	false
197.213.165.206	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
166.177.159.54	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
62.39.174.138	unknown	France		15557	LDCOMNETFR	false
170.126.124.114	unknown	United States		23486	NETSPANUS	false
197.123.112.50	unknown	Egypt		36992	ETISALAT-MISREG	false
41.202.14.230	unknown	Ghana		36961	ZIPNETGH	false
98.224.26.31	unknown	United States		7922	COMCAST-7922US	false
146.71.165.169	unknown	United States		32904	KAJEET-ARTERRA-OTARRISUS	false
41.118.208.5	unknown	South Africa		16637	MTNNS-ASZA	false
167.224.54.93	unknown	United States		2897	GEORGIA-1US	false
97.225.36.41	unknown	United States		6167	CELLCO-PARTUS	false
59.75.35.76	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
156.111.211.46	unknown	United States		395139	NYP-INTERNETUS	false
156.73.167.244	unknown	United States		2024	NUUS	false
41.203.88.59	unknown	Nigeria		37148	globacom-asNG	false
74.222.101.219	unknown	United States		20257	FTC-INETUS	false
156.7.48.43	unknown	United States		29975	VODACOM-ZA	false
41.70.121.242	unknown	Malawi		37098	globe-asMW	false
195.113.207.9	unknown	Czech Republic		2852	CESNET2CZ	false
41.114.27.101	unknown	South Africa		16637	MTNNS-ASZA	false
42.166.168.45	unknown	China		4249	LILLY-ASUS	false
43.126.20.218	unknown	Japan		4249	LILLY-ASUS	false
156.96.125.239	unknown	United States		64249	ENDOFFICEUS	false
156.72.152.79	unknown	United States		29975	VODACOM-ZA	false
197.173.155.16	unknown	South Africa		37168	CELL-CZA	false
156.102.62.17	unknown	United States		393504	XNSTGCA	false
156.189.23.118	unknown	Egypt		36992	ETISALAT-MISREG	false
41.228.193.68	unknown	Tunisia		37693	TUNISIANATN	false
41.92.95.67	unknown	Morocco		36925	ASMediMA	false
197.168.182.250	unknown	South Africa		37168	CELL-CZA	false
220.5.126.251	unknown	Japan		17676	GIGAINFRASoftbankBBCorp JP	false
197.96.225.174	unknown	South Africa		3741	ISZA	false
23.130.234.85	unknown	Reserved		32242	ULTRA-KINGVG	false
131.228.156.101	unknown	Finland		1248	HERENL	false
41.203.88.45	unknown	Nigeria		37148	globacom-asNG	false
63.237.131.6	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
197.134.36.206	unknown	Egypt		24835	RAYA-ASEG	false
188.90.34.34	unknown	Netherlands		31615	TMO-NL-ASNL	false
101.160.59.76	unknown	Australia		1221	ASN-TELSTRATelstraCorporation LtdAU	false
186.9.217.236	unknown	Chile		27925	EntelPCSTelecomunicacionesSACL	false
92.48.138.84	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
156.107.128.107	unknown	United States		8414	PlacedesNationsCH-1211Geneva20SwitzerlandGR	false
182.203.187.255	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
41.233.34.176	unknown	Egypt		8452	TE-ASTE-ASEG	false
65.107.50.235	unknown	United States		2828	XO-AS15US	false
164.133.129.98	unknown	Germany		16276	OVHFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.41.152.232	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.249.194.178	unknown	Mozambique		25139	TVCABO-ASEU	false
5.137.136.10	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
78.227.115.51	unknown	France		12322	PROXADFR	false
101.95.142.200	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
156.92.204.66	unknown	United States		10695	WAL-MARTUS	false
156.8.64.239	unknown	South Africa		3741	ISZA	false
197.100.219.15	unknown	South Africa		3741	ISZA	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
41.182.10.64	8LdKQIRfZG	Get hash	malicious	Browse	
41.187.159.158	E38HvGUw3W	Get hash	malicious	Browse	
189.215.130.156	YQqx8LTbmF	Get hash	malicious	Browse	
41.216.98.146	KEgx4lC3Ni	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	arm	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.132
	FWsCarsq8Q	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	arm	Get hash	malicious	Browse	• 162.213.33.132
	7qvn4qlmi3	Get hash	malicious	Browse	• 162.213.33.132
	JuofJwjQMT	Get hash	malicious	Browse	• 162.213.33.108
	GRPVtMlbK5	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.132
	lCTNXNa4Bo	Get hash	malicious	Browse	• 162.213.33.132
	JIUq8a4ITS	Get hash	malicious	Browse	• 162.213.33.132
	UniRHdW5VC	Get hash	malicious	Browse	• 162.213.33.108
	5skQ8s2EsJ	Get hash	malicious	Browse	• 162.213.33.132
	mYBcqY8Xlj	Get hash	malicious	Browse	• 162.213.33.132
	KEgx4lC3Ni	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
NOOR-ASEG	PFD33mzc5l	Get hash	malicious	Browse	• 41.187.12.190
	arm.light	Get hash	malicious	Browse	• 197.246.153.217
	x86	Get hash	malicious	Browse	• 41.187.12.174
	mYBcqY8Xlj	Get hash	malicious	Browse	• 41.187.200.111
	KEgx4lC3Ni	Get hash	malicious	Browse	• 41.187.12.195
	sh1i15951l	Get hash	malicious	Browse	• 41.187.159.160
	x.arm7	Get hash	malicious	Browse	• 41.187.159.157
	VdhQknQq9e	Get hash	malicious	Browse	• 41.187.12.179
	yXTRZQmYdr	Get hash	malicious	Browse	• 41.187.12.196
	b3astmode.arm7	Get hash	malicious	Browse	• 197.246.117.163
	0FPjf8qK5E	Get hash	malicious	Browse	• 41.187.200.117

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	D0sF4Fm8Za	Get hash	malicious	Browse	• 41.187.159.136
	arm	Get hash	malicious	Browse	• 41.187.159.153
	8EddA0qHLY	Get hash	malicious	Browse	• 41.187.200.102
	x86	Get hash	malicious	Browse	• 41.187.12.172
	Le85313EpP	Get hash	malicious	Browse	• 41.187.200.114
	46gV91KJhQ	Get hash	malicious	Browse	• 41.187.200.117
	8LdKQlRfZG	Get hash	malicious	Browse	• 41.187.112.140
	N2td06Hra9	Get hash	malicious	Browse	• 197.246.11 7.188
	17Rom1F3MY	Get hash	malicious	Browse	• 41.187.200.106
ALJAWWALSTC-ASSA	arm7	Get hash	malicious	Browse	• 178.86.67.159
	cWoHkWMMOf	Get hash	malicious	Browse	• 95.187.84.236
	nzVVA4qMtn	Get hash	malicious	Browse	• 178.86.67.166
	qF7g4nnHh0	Get hash	malicious	Browse	• 178.86.67.142
	l0uZkpwjxy	Get hash	malicious	Browse	• 178.86.67.170
	UnHAnaAW.arm7	Get hash	malicious	Browse	• 95.187.48.174
	L1ecmEWyAw	Get hash	malicious	Browse	• 178.86.67.114
	666.arm7	Get hash	malicious	Browse	• 178.86.67.156
	b3astmode.arm7	Get hash	malicious	Browse	• 93.169.118.181
	tmDSSwkOAM	Get hash	malicious	Browse	• 37.224.144.205
	Tsunami.arm7	Get hash	malicious	Browse	• 95.186.223.111
	80wVQ9c87m	Get hash	malicious	Browse	• 5.156.68.119
	itdWubrQL9	Get hash	malicious	Browse	• 95.185.43.100
	yir8ieZzXL	Get hash	malicious	Browse	• 178.86.67.161
	OttD031TT2	Get hash	malicious	Browse	• 178.86.67.149
	4uSa8tiph0	Get hash	malicious	Browse	• 5.156.68.178
	H9pNgz5hYJ	Get hash	malicious	Browse	• 95.186.223.119
	sora.arm7	Get hash	malicious	Browse	• 37.224.144.214
	TXPZjZV9Bq.exe	Get hash	malicious	Browse	• 95.185.0.165
	i0YmKTxSjH.exe	Get hash	malicious	Browse	• 95.185.0.165

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8662467bc96db2d387755570446a7946	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
	1isequal9.arm7	Get hash	malicious	Browse	• 162.213.33.132
fb4726d465c5f28b84cd6d14cedd13a7	khoE2I8yer	Get hash	malicious	Browse	• 34.249.145.219
	wvsEoQ0khP	Get hash	malicious	Browse	• 34.249.145.219
	32	Get hash	malicious	Browse	• 34.249.145.219
	a-r.m-5.Sakura	Get hash	malicious	Browse	• 34.249.145.219
	NDYfrLSNFW	Get hash	malicious	Browse	• 34.249.145.219
	m-i.p-s.Sakura	Get hash	malicious	Browse	• 34.249.145.219
	6Qn1b9fB2C	Get hash	malicious	Browse	• 34.249.145.219
	ZSbDircdwC	Get hash	malicious	Browse	• 34.249.145.219
	s0bi9t	Get hash	malicious	Browse	• 34.249.145.219
	E7VXPEy1i2	Get hash	malicious	Browse	• 34.249.145.219

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JIMFLthThO	Get hash	malicious	Browse	• 34.249.145.219
	[cpu]	Get hash	malicious	Browse	• 34.249.145.219
	vC6OApPu6u	Get hash	malicious	Browse	• 34.249.145.219
	i686	Get hash	malicious	Browse	• 34.249.145.219
	4f0PBbcOBI	Get hash	malicious	Browse	• 34.249.145.219
	7iw4z5l41w	Get hash	malicious	Browse	• 34.249.145.219
	SecuriteInfo.com.PUA.Tool.Linux.BtcMine.2805.26628.5655	Get hash	malicious	Browse	• 34.249.145.219
	SecuriteInfo.com.Application.Linux.Generic.8393.27.2764	Get hash	malicious	Browse	• 34.249.145.219
	SecuriteInfo.com.MacOS.Miner-ERPUP.18192.8301	Get hash	malicious	Browse	• 34.249.145.219
	SecuriteInfo.com.Trojan.Linux.Generic.190708.11930.2118	Get hash	malicious	Browse	• 34.249.145.219

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/5321/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

/proc/5321/oom_score_adj	
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 -1000.

/proc/5380/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/5383/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/5385/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/5387/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

/proc/5387/oom_score_adj	
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/5389/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/5391/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/5396/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/5544/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped

/proc/5544/oom_score_adj	
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

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

/proc/5577/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/5579/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/5581/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)

/proc/5581/oom_score_adj	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5583/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/5585/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/5588/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/5852/oom_score_adj	
Process:	/usr/bin/dbus-daemon

/proc/5852/oom_score_adj	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5998/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/6118/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/6181/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:DXUv:L2
MD5:	7D46BB41C8CFCB3AC0ED243C99FC9752
SHA1:	214D76314871D1059A73E0D473EE2E0AE8A74D08
SHA-256:	842CE7718CA1D8B306A3857F7CFC00A8F005E147869EE225935231B271281A83
SHA-512:	77A53FA4C43B38EB9AB717F498D051EAA09717407BE2DC1BBCCA5267F545BEA01163BA58F982FBD4EA0FB6BDB4D366D3951F359B77F58C4D941A9B3301D25B 5
Malicious:	false
Preview:	 5321.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:Exv:Exv
MD5:	EE532C893137A109ECCFE747D14B70C6
SHA1:	82B0A0E5CC7304DCFC72C132D3440AA8E998AD57
SHA-256:	C1144A9FE5BE45FC50E882FFD319A5C531D5076075346F771A3570410736E3A2
SHA-512:	DF6D818F530F0B8EBBEB667337E85B13EED4FA5D9DA30375FD953EBF1DEC71C0D9B6F75F35CB5CCC926417E7DB2A97CD98E8CF9C1FDE006AB559D9E393696 999
Malicious:	false
Preview:	 5442.

/run/user/127/ICEauthority	
Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	5.997673931787549
Encrypted:	false
SSDEEP:	12:OxPjYW1OveY+jYFOxP7MaDveY+7LbimxP5mhijveY+5tWmxPwWoveY+wcZVveY+n:6Wo7AwqrqHl+
MD5:	E385125478061975C376B279FB3A22A2
SHA1:	DE16305100EDC06A69C86A817FA17E5B04BCB3AB
SHA-256:	E8B994276FE181F052CC23CEAC124D71E98B0C15314B2D1B1C26702D24A4E609
SHA-512:	B3804AFAAD86F739F3F9FC04DFAD74555ED1BC8745B50EA286C9A058330C773726E454659E7615F10FC4C9DCB9674D6FE9A27187F7C2B9F2039F7DA17A321F1
Malicious:	false
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5528..MIT-MAGIC-COOKIE-1.....lut...O#X.._..XSMP...#local/galassia:@/tmp/.ICE-unix/5528..MIT-MAGIC-COOKIE-1..X.....:.TD8e N....ICE...!unix/galassia:/tmp/.ICE-unix/5376..MIT-MAGIC-COOKIE-1..e.X3.)2U..3a..R..ICE...#local/galassia:@/tmp/.ICE-unix/5376..MIT-MAGIC-COOKIE-1.....c..K. .....XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.....A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....o.(R...} .9...ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f.....E ..c..XSMP...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... .....Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,.:B .o.....ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte\|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN... ..N+..$..XSMP...#local/galass

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

/run/user/127/dconf/user	
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):	4.882427239163554
Encrypted:	false
SSDEEP:	3:rg/WFllasO93MZHMYitWFllasO93MZHMd:rg/WFl2htWFl2X
MD5:	5E12994A988CFEA541E152F605AE8129
SHA1:	973A78EA1F7841E94893E72A90E566EBC61E33DF
SHA-256:	8BE397CFD980E95390B269B99F951705B21EAB7444540B0086520660CDDCC515
SHA-512:	06C39FCAA9812BA506DFB75C8913BAA8B4D27B8F6559C791483B8F6A187027A51154D49D522EB54153907D68B6211110B16E2064240D5F9265E11737E2943E8B
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1....^.b.2]...ll.....galassia....MIT-MAGIC-COOKIE-1....^.b.2]...ll.

/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:JVWv:bo
MD5:	FB873011BE6F1329587A211E689D51BC
SHA1:	CB300A2A7A3D46AF1325144C3C80BCCE0BDF76EA
SHA-256:	E61D6291032BBB893A20E74366CE8055CF3823F450876A315B6D842BD861EA5E
SHA-512:	C868E99D74D233B0950BC0F825413A09BCCF5B3411763D8D2E03F5E11B4F6BA38E240DABE4B0ADA39AABAC629A2107E6DE574A101CF758DBFBAC2FFBE0811413
Malicious:	false
Preview:	5903.

/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:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE001
Malicious:	false
Preview:	.mkx.....D.....h.....<.....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWNPGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFINDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18

/var/cache/motd-news	
Process:	/usr/bin/cut
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.515771857099866
Encrypted:	false

/var/cache/motd-news	
SSDEEP:	3:P2lnI+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn
MD5:	DD514F892B5F93ED615D366E58AC58AF
SHA1:	BA75EDB3C2232CC260BC187F604DC8F25AA72C11
SHA-256:	F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF
SHA-512:	9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACCDBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42A2D0
Malicious:	false
Preview:	* Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation.

/var/lib/AccountsService/users/gdm.1KK0B1	
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:gzMQlzKLrAa4M
MD5:	542BA3FB41206AE43928AF1C5E61FEBC
SHA1:	F56F574DAF50D609526B36B5B54FDD59EA4D6A26
SHA-256:	730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A
SHA-512:	D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42FAEA
Malicious:	false
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/AccountsService/users/gdm.H81KB1	
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:gzMQlzKLrAa4M
MD5:	542BA3FB41206AE43928AF1C5E61FEBC
SHA1:	F56F574DAF50D609526B36B5B54FDD59EA4D6A26
SHA-256:	730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A
SHA-512:	D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42FAEA
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):	5.141274097369678
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWV6NdehKhp8:q5sU3LWfLUDmQymqSFbfomSuGKXfKvn
MD5:	577100A53078679681CE31B115A0EC7B
SHA1:	E2F125E4B5663FE88EEE74AF86BA46E778142FD6
SHA-256:	A7A948E3B9228CA93AE7E39ADB8986564200E561411C9833113DDDC9B1C62D53
SHA-512:	6276A85026838DFFDE7160322B9DD7BCB435A65D8E945A8CB7F77E81868DED95CAF6ABFC10045316943279F45CA0181CFAA92400DA48FAE8B075BA31F342D11
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-Ds0pDrdp,guid=99d95171f4dc385ddc2326286170cac3.IBUS_DAEMON_PID=5648.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
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/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.K47ZB1	
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):	5.2940877052748565
Encrypted:	false
SSDEEP:	384:FDywRYQf3xM/dcdRdqd4djdydud5d5d5dFdOdXd3dtdIdldNd2djd2Sd3XdrUd/1:xywjaqxWXkKVa0CIpN6bQ/VA
MD5:	DEE0AAC82ED6F604139C8402FCFC51E5
SHA1:	F4690600D4584C85218422AD1720085AAB45606D
SHA-256:	9B851DFE5ED22B9B583939B7DEA3225A8409B109C66DB4A43BCD57DBD5B6F3E9
SHA-512:	160B5C422487910932BD51D7BD5FE39046BB56469D933205A6247F6B9E2904CF5FEF5756890A8CB58ABAB8996495C0D0AA09AB465ACA4EA885D85D2F19B021B5
Malicious:	false
Preview:	[487.473] (--) Log file renamed from "/var/log/Xorg.pid-5435.log" to "/var/log/Xorg.0.log".[487.489] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[4 87.497] Build Operating System: linux Ubuntu.[487.502] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[487.508] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[487.5 22] Build Date: 06 July 2021 10:17:51AM.[487.531] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[487.535] Current version of pixman: 0.38.4.[487.539] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[487.543] 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):	7.986971107522109
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm7
File size:	70904
MD5:	1adc0d120624cd12b4546ad9815857a8
SHA1:	5e17dd426d0d53dceed208de50c494f27eee8e10
SHA256:	3cd04e2c688f17b1da70b441a5db1bdd254f4f3a44c7e9e76df944eaa7cde275
SHA512:	4240b8c0314e7e1c79d0681a73e13f2ad1f6ebe43c834c4cb24194ceb966f1f62f60efa0c4b604f38ad116881bb0672a217771d013811623c0e876ee2f65d1c1
SSDEEP:	1536:6OFSklNkKCM6VXsFcAe2KERzQfkObIG5bL1sCEhi0cMonSh3:6OFSMQMbcAIx8QIG5bL2CDnMonSN
File Content Preview:	.ELF.....(.....X<..4.....4. ...(.....E...E.....V...V...V.....Q.td.....aUPX!.....m.....?.E.h;....#..$...o..,_...sl.....?.z..vc.s..g7.U.....!..G....b..

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:	0x13c58
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	0xce45	0xce45	4.0211	0x5	R E	0x8000		
LOAD	0x5614	0x35614	0x35614	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
Oct 21, 2021 02:03:32.617383957 CEST	192.168.2.23	1.1.1.1	0x29df	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 21, 2021 02:03:32.617459059 CEST	192.168.2.23	1.1.1.1	0xd835	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Oct 21, 2021 02:03:32.715140104 CEST	192.168.2.23	1.1.1.1	0xf4a3	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
Oct 21, 2021 02:03:32.634016991 CEST	1.1.1.1	192.168.2.23	0x29df	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Oct 21, 2021 02:03:32.634016991 CEST	1.1.1.1	192.168.2.23	0x29df	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: arm7 PID: 5231 Parent PID: 5109

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	/tmp/arm7
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: arm7 PID: 5233 Parent PID: 5231

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5235 Parent PID: 5231

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5236 Parent PID: 5231

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5240 Parent PID: 5231

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5241 Parent PID: 5231

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5244 Parent PID: 5231

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5247 Parent PID: 5244

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5250 Parent PID: 5244

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5252 Parent PID: 5250

General

Start time:	02:02:46
Start date:	21/10/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5291 Parent PID: 1

General

Start time:	02:03:31
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5291 Parent PID: 1

General

Start time:	02:03:31
Start date:	21/10/2021
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: 5320 Parent PID: 1

General

Start time:	02:03:35
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5320 Parent PID: 1

General

Start time:	02:03:35
Start date:	21/10/2021
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: 5321 Parent PID: 1

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5321 Parent PID: 1

General

Start time:	02:03:36

Start date:	21/10/2021
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: dash PID: 5322 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5322 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.ufH0NYtBX2
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5323 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5323 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5324 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5324 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5325 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5325 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/cut

Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5326 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5326 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.ufH0NYtBX2
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5327 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5327 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5328 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5328 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5329 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5329 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: dash PID: 5330 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5330 Parent PID: 4333

General

Start time:	02:03:36
Start date:	21/10/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.ufH0NYtBX2 /tmp/tmp.4U2ZRxJPEO /tmp/tmp.Q0Nrki22iD
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: gdm3 PID: 5337 Parent PID: 1320

General

Start time:	02:03:43
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5337 Parent PID: 1320

General

Start time:	02:03:43
Start date:	21/10/2021
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: 5340 Parent PID: 1320

General

Start time:	02:03:43
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5340 Parent PID: 1320

General

Start time:	02:03:43
Start date:	21/10/2021
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: 5341 Parent PID: 1

General

Start time:	02:03:43
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5341 Parent PID: 1

General

Start time:	02:03:43
Start date:	21/10/2021
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: 5360 Parent PID: 5341

General

Start time:	02:03:43
Start date:	21/10/2021
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: 5360 Parent PID: 5341

General

Start time:	02:03:43
Start date:	21/10/2021
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: 5361 Parent PID: 5360

General

Start time:	02:03:43
Start date:	21/10/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5361 Parent PID: 5360

General

Start time:	02:03:43
Start date:	21/10/2021
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: 5362 Parent PID: 5361

General

Start time:	02:03:44
Start date:	21/10/2021
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5362 Parent PID: 5361

General

Start time:	02:03:44
Start date:	21/10/2021
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: 5363 Parent PID: 5362

General

Start time:	02:03:44
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5363 Parent PID: 5362

General

Start time:	02:03:44
Start date:	21/10/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5364 Parent PID: 5362

General

Start time:	02:03:44
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5364 Parent PID: 5362

General

Start time:	02:03:44
Start date:	21/10/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gdm3 PID: 5365 Parent PID: 1320

General

Start time:	02:03:46
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5365 Parent PID: 1320

General

Start time:	02:03:46
Start date:	21/10/2021
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: 5371 Parent PID: 5365

General

Start time:	02:03:48
Start date:	21/10/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 5371 Parent PID: 5365

General

Start time:	02:03:48
Start date:	21/10/2021
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: 5374 Parent PID: 5371

General

Start time:	02:03:48
Start date:	21/10/2021
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: 5374 Parent PID: 5371

General

Start time:	02:03:48
Start date:	21/10/2021
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: 5375 Parent PID: 5374

General

Start time:	02:03:48
Start date:	21/10/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

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

General

Start time:	02:03:48
Start date:	21/10/2021
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: 5379 Parent PID: 5375

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5380 Parent PID: 5379

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5380 Parent PID: 5379

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5382 Parent PID: 5375

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5383 Parent PID: 5382

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon

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

File Activities

File Written

Analysis Process: false PID: 5383 Parent PID: 5382

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5384 Parent PID: 5375

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5385 Parent PID: 5384

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5385 Parent PID: 5384

General

Start time:	02:03:50

Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5386 Parent PID: 5375

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5387 Parent PID: 5386

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5387 Parent PID: 5386

General

Start time:	02:03:50
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5388 Parent PID: 5375

General

Start time:	02:03:51
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5389 Parent PID: 5388

General

Start time:	02:03:51
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5389 Parent PID: 5388

General

Start time:	02:03:51
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5390 Parent PID: 5375

General

Start time:	02:03:51
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5391 Parent PID: 5390

General

Start time:	02:03:51
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon

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

File Activities

File Written

Analysis Process: false PID: 5391 Parent PID: 5390

General

Start time:	02:03:52
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5395 Parent PID: 5375

General

Start time:	02:03:52
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5396 Parent PID: 5395

General

Start time:	02:03:52
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5396 Parent PID: 5395

General

Start time:	02:03:52

Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5376 Parent PID: 5374

General

Start time:	02:03:49
Start date:	21/10/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5376 Parent PID: 5374

General

Start time:	02:03:49
Start date:	21/10/2021
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: 5376 Parent PID: 5374

General

Start time:	02:03:49
Start date:	21/10/2021
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: 5397 Parent PID: 5376

General

Start time:	02:03:53
Start date:	21/10/2021
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: 5397 Parent PID: 5376

General

Start time:	02:03:53
Start date:	21/10/2021
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: 5398 Parent PID: 5376

General

Start time:	02:03:54
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5398 Parent PID: 5376

General

Start time:	02:03:54
Start date:	21/10/2021
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: 5398 Parent PID: 5376

General

Start time:	02:03:54
Start date:	21/10/2021
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: 5426 Parent PID: 1320

General

Start time:	02:03:58
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5426 Parent PID: 1320

General

Start time:	02:03:58
Start date:	21/10/2021
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: 5431 Parent PID: 5426

General

Start time:	02:03:59
Start date:	21/10/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 5431 Parent PID: 5426

General

Start time:	02:03:59
Start date:	21/10/2021
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: 5435 Parent PID: 5431

General

Start time:	02:04:00
Start date:	21/10/2021
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: 5435 Parent PID: 5431

General

Start time:	02:04:00
Start date:	21/10/2021

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: 5435 Parent PID: 5431

General

Start time:	02:04:00
Start date:	21/10/2021
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: 5435 Parent PID: 5431

General

Start time:	02:04:00
Start date:	21/10/2021
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: 5476 Parent PID: 5435

General

Start time:	02:04:12
Start date:	21/10/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes

MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5476 Parent PID: 5435

General

Start time:	02:04:12
Start date:	21/10/2021
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: 5477 Parent PID: 5476

General

Start time:	02:04:12
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5477 Parent PID: 5476

General

Start time:	02:04:12
Start date:	21/10/2021
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: 5898 Parent PID: 5435

General

Start time:	02:04:53
Start date:	21/10/2021

Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5898 Parent PID: 5435

General

Start time:	02:04:53
Start date:	21/10/2021
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: 5900 Parent PID: 5898

General

Start time:	02:04:53
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5900 Parent PID: 5898

General

Start time:	02:04:53
Start date:	21/10/2021
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: 5525 Parent PID: 5431

General

General

Start time:	02:04:23
Start date:	21/10/2021
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: 5525 Parent PID: 5431

General

Start time:	02:04:23
Start date:	21/10/2021
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: 5526 Parent PID: 5431

General

Start time:	02:04:23
Start date:	21/10/2021
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: 5526 Parent PID: 5431

General

Start time:	02:04:23
Start date:	21/10/2021
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: 5527 Parent PID: 5526

General

Start time:	02:04:23
Start date:	21/10/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5527 Parent PID: 5526

General

Start time:	02:04:23
Start date:	21/10/2021
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: 5543 Parent PID: 5527

General

Start time:	02:04:31
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5544 Parent PID: 5543

General

Start time:	02:04:31
Start date:	21/10/2021
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: 5544 Parent PID: 5543

General

Start time:	02:04:31
Start date:	21/10/2021
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: 5549 Parent PID: 5544

General

Start time:	02:04:31
Start date:	21/10/2021
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: 5549 Parent PID: 5544

General

Start time:	02:04:31
Start date:	21/10/2021
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: 5994 Parent PID: 5549

General

Start time:	02:04:57
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5998 Parent PID: 5994

General

Start time:	02:04:57
Start date:	21/10/2021
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: 5998 Parent PID: 5994

General

Start time:	02:04:57
Start date:	21/10/2021
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: 5573 Parent PID: 5527

General

Start time:	02:04:34
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

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

General

Start time:	02:04:34
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5574 Parent PID: 5573

General

Start time:	02:04:34
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5576 Parent PID: 5527

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5577 Parent PID: 5576

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5577 Parent PID: 5576

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5578 Parent PID: 5527

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5579 Parent PID: 5578

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5579 Parent PID: 5578

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5580 Parent PID: 5527

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5581 Parent PID: 5580

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5581 Parent PID: 5580

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5582 Parent PID: 5527

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5583 Parent PID: 5582

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5583 Parent PID: 5582

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5584 Parent PID: 5527

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5585 Parent PID: 5584

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5585 Parent PID: 5584

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5587 Parent PID: 5527

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5588 Parent PID: 5587

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5588 Parent PID: 5587

General

Start time:	02:04:35
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5848 Parent PID: 5527

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5852 Parent PID: 5848

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: ibus-portal PID: 5852 Parent PID: 5848

General

Start time:	02:04:51
Start date:	21/10/2021
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: 6117 Parent PID: 5527

General

Start time:	02:04:59
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon

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

Analysis Process: dbus-daemon PID: 6118 Parent PID: 6117

General

Start time:	02:04:59
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: gjs PID: 6118 Parent PID: 6117

General

Start time:	02:04:59
Start date:	21/10/2021
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: 6180 Parent PID: 5527

General

Start time:	02:05:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 6181 Parent PID: 6180

General

Start time:	02:05:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon

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

File Activities

File Written

Analysis Process: false PID: 6181 Parent PID: 6180

General

Start time:	02:05:13
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5528 Parent PID: 5526

General

Start time:	02:04:24
Start date:	21/10/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5528 Parent PID: 5526

General

Start time:	02:04:24
Start date:	21/10/2021
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: 5528 Parent PID: 5526

General

Start time:	02:04:24

Start date:	21/10/2021
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: 5529 Parent PID: 5528

General

Start time:	02:04:25
Start date:	21/10/2021
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: 5529 Parent PID: 5528

General

Start time:	02:04:25
Start date:	21/10/2021
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: 5550 Parent PID: 5529

General

Start time:	02:04:31
Start date:	21/10/2021
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: 5550 Parent PID: 5529

General

Start time:	02:04:31
Start date:	21/10/2021
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: 5562 Parent PID: 5529

General

Start time:	02:04:33
Start date:	21/10/2021
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: 5562 Parent PID: 5529

General

Start time:	02:04:33
Start date:	21/10/2021
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: 5589 Parent PID: 5528

General

Start time:	02:04:36
Start date:	21/10/2021
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: 5589 Parent PID: 5528

General

Start time:	02:04:36
Start date:	21/10/2021
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: 5590 Parent PID: 5528

General

Start time:	02:04:37
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5590 Parent PID: 5528

General

Start time:	02:04:37
Start date:	21/10/2021
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: 5590 Parent PID: 5528

General

Start time:	02:04:37
Start date:	21/10/2021
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: 5648 Parent PID: 5590

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5648 Parent PID: 5590

General

Start time:	02:04:51
Start date:	21/10/2021
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: 5782 Parent PID: 5648

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5782 Parent PID: 5648

General

Start time:	02:04:51
Start date:	21/10/2021
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: 5814 Parent PID: 5648

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5818 Parent PID: 5814

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5818 Parent PID: 1

General

Start time:	02:04:51
Start date:	21/10/2021
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: 6163 Parent PID: 5648

General

Start time:	02:05:08
Start date:	21/10/2021
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: 6163 Parent PID: 5648

General

Start time:	02:05:09
Start date:	21/10/2021
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: 6139 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6139 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6139 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6141 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6141 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6141 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6143 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6143 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6143 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6144 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6144 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6144 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6145 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6145 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
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: 6145 Parent PID: 5528

General

Start time:	02:05:04
Start date:	21/10/2021
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: 6191 Parent PID: 6145

General

Start time:	02:05:15
Start date:	21/10/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6192 Parent PID: 6191

General

Start time:	02:05:15
Start date:	21/10/2021
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: 6192 Parent PID: 1

General

Start time:	02:05:15
Start date:	21/10/2021
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: 6146 Parent PID: 5528

General

Start time:	02:05:03
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6146 Parent PID: 5528

General

Start time:	02:05:04
Start date:	21/10/2021
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: 6146 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
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: 6147 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6147 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
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: 6147 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
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: 6149 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6149 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
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: 6149 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
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: 6150 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6150 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
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: 6150 Parent PID: 5528

General

Start time:	02:05:06
Start date:	21/10/2021
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: 6151 Parent PID: 5528

General

Start time:	02:05:05
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6151 Parent PID: 5528

General

Start time:	02:05:06
Start date:	21/10/2021
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: 6151 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
Path:	/usr/libexec/gsd-screensaver-proxy
Arguments:	/usr/libexec/gsd-screensaver-proxy
File size:	27232 bytes

MD5 hash:	77e309450c87dceee43f1a9e50cc0d02

Analysis Process: gnome-session-binary PID: 6154 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6154 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gsd-sound PID: 6154 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
Path:	/usr/libexec/gsd-sound
Arguments:	/usr/libexec/gsd-sound
File size:	31248 bytes
MD5 hash:	4c7d3fb993463337b4a0eb5c80c760ee

Analysis Process: gnome-session-binary PID: 6156 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6156 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
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: 6156 Parent PID: 5528

General

Start time:	02:05:09
Start date:	21/10/2021
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: 6161 Parent PID: 5528

General

Start time:	02:05:07
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6161 Parent PID: 5528

General

Start time:	02:05:09
Start date:	21/10/2021
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: 6161 Parent PID: 5528

General

Start time:	02:05:09
Start date:	21/10/2021
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

Analysis Process: gnome-session-binary PID: 6164 Parent PID: 5528

General

Start time:	02:05:09

Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6164 Parent PID: 5528

General

Start time:	02:05:09
Start date:	21/10/2021
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: 6164 Parent PID: 5528

General

Start time:	02:05:09
Start date:	21/10/2021
Path:	/usr/libexec/gsd-power
Arguments:	/usr/libexec/gsd-power
File size:	88672 bytes
MD5 hash:	28b8e1b43c3e7f1db6741ea1ecd978b7

Analysis Process: gnome-session-binary PID: 7032 Parent PID: 5528

General

Start time:	02:05:40
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 7032 Parent PID: 5528

General

Start time:	02:05:40
Start date:	21/10/2021
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: 7032 Parent PID: 5528

General

Start time:	02:05:40
Start date:	21/10/2021
Path:	/usr/bin/spice-vdagent
Arguments:	/usr/bin/spice-vdagent
File size:	80664 bytes
MD5 hash:	80fb7f613aa78d1b8a229dbcf4577a9d

Analysis Process: gnome-session-binary PID: 7039 Parent PID: 5528

General

Start time:	02:05:42
Start date:	21/10/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 7039 Parent PID: 5528

General

Start time:	02:05:42
Start date:	21/10/2021
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: 7039 Parent PID: 5528

General

Start time:	02:05:44
Start date:	21/10/2021
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5427 Parent PID: 1320

General

Start time:	02:03:58
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5427 Parent PID: 1320

General

Start time:	02:03:58
Start date:	21/10/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5428 Parent PID: 1320

General

Start time:	02:03:58
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5428 Parent PID: 1320

General

Start time:	02:03:58
Start date:	21/10/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5436 Parent PID: 1320

General

Start time:	02:04:01
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5436 Parent PID: 1320

General

Start time:	02:04:01
Start date:	21/10/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemd PID: 5442 Parent PID: 1860

General

Start time:	02:04:06
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5442 Parent PID: 1860

General

Start time:	02:04:06
Start date:	21/10/2021
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: 5482 Parent PID: 2038

General

Start time:	02:04:19
Start date:	21/10/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5482 Parent PID: 2038

General

Start time:	02:04:19
Start date:	21/10/2021
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

Analysis Process: systemd PID: 5500 Parent PID: 1

General

Start time:	02:04:22
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5500 Parent PID: 1

General

Start time:	02:04:22
Start date:	21/10/2021
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: 5615 Parent PID: 1

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5615 Parent PID: 1

General

Start time:	02:04:51
Start date:	21/10/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 5903 Parent PID: 1334

General

Start time:	02:04:55
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5903 Parent PID: 1334

General

Start time:	02:04:55
Start date:	21/10/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5906 Parent PID: 1

General

Start time:	02:04:57
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5906 Parent PID: 1

General

Start time:	02:04:57
Start date:	21/10/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 6193 Parent PID: 1

General

Start time:	02:05:16
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-hostnamed PID: 6193 Parent PID: 1

General

Start time:	02:05:16
Start date:	21/10/2021
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	35040 bytes
MD5 hash:	2cc8a5576629a2d5bd98e49a4b8bef65

Analysis Process: systemd PID: 6548 Parent PID: 1

General

Start time:	02:05:32
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 6548 Parent PID: 1

General

Start time:	02:05:32
Start date:	21/10/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 6813 Parent PID: 1

General

Start time:	02:05:35
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6813 Parent PID: 1

General

Start time:	02:05:35
Start date:	21/10/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84