JoeSandbox Cloud BASIC

ID: 506687
Sample Name: uwgXkY20gB
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:06:41
Date: 21/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Linux Analysis Report uwgXkY20gB

Overview

General Information

Sample Name:	uwgXkY20gB
Analysis ID:	506687
MD5:	949c3108afe02ab.
SHA1:	b0fa61c619dfa80..
SHA256:	f620d815094fa7c..
Tags:	32 elf gafgyt renesas
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

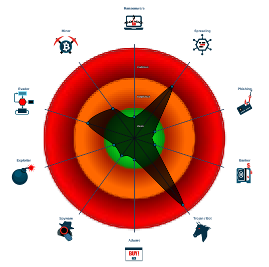
Mirai

Score:	92
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…
- Uses known network protocols on no…
- Sample reads /proc/mounts (often u…
- Reads CPU information from /sys in…
- Executes the "grep" command used…
- Uses the "uname" system call to qu…
- Enumerates processes within the "p

Classification



Analysis Advice

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:	506687
Start date:	21.10.2021
Start time:	02:06:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uwgXkY20gB
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:	mal92.spre.troj.lin@0/52@3/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- uwgXkY20gB (PID: 5237, Parent: 5111, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/uwgXkY20gB
  - uwgXkY20gB New Fork (PID: 5239, Parent: 5237)
  - uwgXkY20gB New Fork (PID: 5240, Parent: 5237)
  - uwgXkY20gB New Fork (PID: 5241, Parent: 5237)
  - uwgXkY20gB New Fork (PID: 5243, Parent: 5237)
  - uwgXkY20gB New Fork (PID: 5244, Parent: 5237)
  - uwgXkY20gB New Fork (PID: 5248, Parent: 5237)
    - uwgXkY20gB New Fork (PID: 5251, Parent: 5248)
    - uwgXkY20gB New Fork (PID: 5253, Parent: 5248)
      - uwgXkY20gB New Fork (PID: 5255, Parent: 5253)

- dash New Fork (PID: 5275, Parent: 4331)
- cat (PID: 5275, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.f7vJ3oarTQ
- dash New Fork (PID: 5276, Parent: 4331)
- head (PID: 5276, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5277, Parent: 4331)
- tr (PID: 5277, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5278, Parent: 4331)
- cut (PID: 5278, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5279, Parent: 4331)
- cat (PID: 5279, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.f7vJ3oarTQ
- dash New Fork (PID: 5280, Parent: 4331)
- head (PID: 5280, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5281, Parent: 4331)
- tr (PID: 5281, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5282, Parent: 4331)
- cut (PID: 5282, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5285, Parent: 4331)
- rm (PID: 5285, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.f7vJ3oarTQ /tmp/tmp.mQ9Xgt5KVB /tmp/tmp.SEXT8WVCCo
- systemd New Fork (PID: 5304, Parent: 1)
- whoopsie (PID: 5304, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5315, Parent: 1)
- sshd (PID: 5315, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5320, Parent: 1)
- sshd (PID: 5320, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5323, Parent: 1320)
- Default (PID: 5323, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5326, Parent: 1320)
- Default (PID: 5326, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5327, Parent: 1)
- accounts-daemon (PID: 5327, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5349, Parent: 5327)
  - language-validate (PID: 5349, Parent: 5327, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5350, Parent: 5349)
    - language-options (PID: 5350, Parent: 5349, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5351, Parent: 5350)
      - sh (PID: 5351, Parent: 5350, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5352, Parent: 5351)
        - locale (PID: 5352, Parent: 5351, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5353, Parent: 5351)
        - grep (PID: 5353, Parent: 5351, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm3 New Fork (PID: 5356, Parent: 1320)
- gdm-session-worker (PID: 5356, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5360, Parent: 5356)
  - gdm-wayland-session (PID: 5360, Parent: 5356, 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: 5363, Parent: 5360)
    - dbus-run-session (PID: 5363, Parent: 5360, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
      - dbus-run-session New Fork (PID: 5364, Parent: 5363)
      - dbus-daemon (PID: 5364, Parent: 5363, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5368, Parent: 5364)
          - dbus-daemon New Fork (PID: 5369, Parent: 5368)
          - false (PID: 5369, Parent: 5368, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5371, Parent: 5364)
          - dbus-daemon New Fork (PID: 5372, Parent: 5371)
          - false (PID: 5372, Parent: 5371, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5373, Parent: 5364)
          - dbus-daemon New Fork (PID: 5374, Parent: 5373)
          - false (PID: 5374, Parent: 5373, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5375, Parent: 5364)
          - dbus-daemon New Fork (PID: 5376, Parent: 5375)
          - false (PID: 5376, Parent: 5375, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5377, Parent: 5364)
          - dbus-daemon New Fork (PID: 5378, Parent: 5377)
          - false (PID: 5378, Parent: 5377, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5379, Parent: 5364)
          - dbus-daemon New Fork (PID: 5380, Parent: 5379)
          - false (PID: 5380, Parent: 5379, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5384, Parent: 5364)
          - dbus-daemon New Fork (PID: 5385, Parent: 5384)
          - false (PID: 5385, Parent: 5384, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - dbus-run-session New Fork (PID: 5365, Parent: 5363)
      - gnome-session (PID: 5365, Parent: 5363, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
      - gnome-session-binary (PID: 5365, Parent: 5363, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary New Fork (PID: 5386, Parent: 5365)
        - session-migration (PID: 5386, Parent: 5365, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
        - gnome-session-binary New Fork (PID: 5387, Parent: 5365)
        - sh (PID: 5387, Parent: 5365, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
        - gnome-shell (PID: 5387, Parent: 5365, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5413, Parent: 1320)
- gdm-session-worker (PID: 5413, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5420, Parent: 5413)
  - gdm-x-session (PID: 5420, Parent: 5413, 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: 5422, Parent: 5420)
    - Xorg (PID: 5422, Parent: 5420, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg.wrap (PID: 5422, Parent: 5420, 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: 5422, Parent: 5420, 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: 5460, Parent: 5422)
    - sh (PID: 5460, Parent: 5422, 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: 5461, Parent: 5460)
        - xkbcomp (PID: 5461, Parent: 5460, 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: 5887, Parent: 5422)
    - sh (PID: 5887, Parent: 5422, 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: 5888, Parent: 5887)
        - xkbcomp (PID: 5888, Parent: 5887, 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: 5469, Parent: 5420)
- Default (PID: 5469, Parent: 5420, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
- gdm-x-session New Fork (PID: 5470, Parent: 5420)
- dbus-run-session (PID: 5470, Parent: 5420, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
    - dbus-run-session New Fork (PID: 5471, Parent: 5470)
    - dbus-daemon (PID: 5471, Parent: 5470, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5532, Parent: 5471)
            - dbus-daemon New Fork (PID: 5533, Parent: 5532)
            - at-spi-bus-launcher (PID: 5533, Parent: 5532, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
                - at-spi-bus-launcher New Fork (PID: 5538, Parent: 5533)
                - dbus-daemon (PID: 5538, Parent: 5533, 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: 5897, Parent: 5538)
                        - dbus-daemon New Fork (PID: 5898, Parent: 5897)
                        - at-spi2-registryd (PID: 5898, Parent: 5897, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
        - dbus-daemon New Fork (PID: 5560, Parent: 5471)
            - dbus-daemon New Fork (PID: 5561, Parent: 5560)
            - false (PID: 5561, Parent: 5560, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5563, Parent: 5471)
            - dbus-daemon New Fork (PID: 5564, Parent: 5563)
            - false (PID: 5564, Parent: 5563, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5567, Parent: 5471)
            - dbus-daemon New Fork (PID: 5568, Parent: 5567)
            - false (PID: 5568, Parent: 5567, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5569, Parent: 5471)
            - dbus-daemon New Fork (PID: 5570, Parent: 5569)
            - false (PID: 5570, Parent: 5569, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5571, Parent: 5471)
            - dbus-daemon New Fork (PID: 5572, Parent: 5571)
            - false (PID: 5572, Parent: 5571, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5573, Parent: 5471)
            - 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: 5471)
            - dbus-daemon New Fork (PID: 5577, Parent: 5576)
            - false (PID: 5577, Parent: 5576, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5883, Parent: 5471)
            - dbus-daemon New Fork (PID: 5884, Parent: 5883)
            - ibus-portal (PID: 5884, Parent: 5883, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
        - dbus-daemon New Fork (PID: 6118, Parent: 5471)
            - dbus-daemon New Fork (PID: 6119, Parent: 6118)
            - gjs (PID: 6119, Parent: 6118, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
        - dbus-daemon New Fork (PID: 6181, Parent: 5471)
            - dbus-daemon New Fork (PID: 6182, Parent: 6181)
            - false (PID: 6182, Parent: 6181, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-run-session New Fork (PID: 5472, Parent: 5470)
    - gnome-session (PID: 5472, Parent: 5470, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
    - gnome-session-binary (PID: 5472, Parent: 5470, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary New Fork (PID: 5473, Parent: 5472)
        - gnome-session-check-accelerated (PID: 5473, Parent: 5472, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
            - gnome-session-check-accelerated New Fork (PID: 5539, Parent: 5473)
            - gnome-session-check-accelerated-gl-helper (PID: 5539, Parent: 5473, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
            - gnome-session-check-accelerated New Fork (PID: 5549, Parent: 5473)
            - gnome-session-check-accelerated-gles-helper (PID: 5549, Parent: 5473, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
        - gnome-session-binary New Fork (PID: 5578, Parent: 5472)
        - session-migration (PID: 5578, Parent: 5472, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
        - gnome-session-binary New Fork (PID: 5579, Parent: 5472)
        - sh (PID: 5579, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
        - gnome-shell (PID: 5579, Parent: 5472, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
            - gnome-shell New Fork (PID: 5630, Parent: 5579)
            - ibus-daemon (PID: 5630, Parent: 5579, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
                - ibus-daemon New Fork (PID: 5879, Parent: 5630)
                - ibus-memconf (PID: 5879, Parent: 5630, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
                - ibus-daemon New Fork (PID: 5881, Parent: 5630)
                    - ibus-daemon New Fork (PID: 5882, Parent: 5881)
                    - ibus-x11 (PID: 5882, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
                - ibus-daemon New Fork (PID: 6154, Parent: 5630)
                - ibus-engine-simple (PID: 6154, Parent: 5630, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
        - gnome-session-binary New Fork (PID: 6136, Parent: 5472)
        - sh (PID: 6136, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec

\"$@\"" sh /usr/libexec/gsd-sharing

- gsd-sharing (PID: 6136, Parent: 5472, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
- gnome-session-binary New Fork (PID: 6138, Parent: 5472)
- sh (PID: 6138, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
- gsd-wacom (PID: 6138, Parent: 5472, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 6140, Parent: 5472)
- sh (PID: 6140, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
- gsd-color (PID: 6140, Parent: 5472, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 6141, Parent: 5472)
- sh (PID: 6141, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
- gsd-keyboard (PID: 6141, Parent: 5472, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 6142, Parent: 5472)
- sh (PID: 6142, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
- gsd-print-notifications (PID: 6142, Parent: 5472, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
  - gsd-print-notifications New Fork (PID: 6462, Parent: 6142)
    - gsd-print-notifications New Fork (PID: 6463, Parent: 6462)
    - gsd-printer (PID: 6463, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 6143, Parent: 5472)
- sh (PID: 6143, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
- gsd-rfkill (PID: 6143, Parent: 5472, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6145, Parent: 5472)
- sh (PID: 6145, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
- gsd-smartcard (PID: 6145, Parent: 5472, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6146, Parent: 5472)
- sh (PID: 6146, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
- gsd-datetime (PID: 6146, Parent: 5472, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6149, Parent: 5472)
- sh (PID: 6149, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
- gsd-media-keys (PID: 6149, Parent: 5472, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6153, Parent: 5472)
- sh (PID: 6153, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
- gsd-screensaver-proxy (PID: 6153, Parent: 5472, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6156, Parent: 5472)
- sh (PID: 6156, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
- gsd-sound (PID: 6156, Parent: 5472, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6157, Parent: 5472)
- sh (PID: 6157, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
- gsd-a11y-settings (PID: 6157, Parent: 5472, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6162, Parent: 5472)
- sh (PID: 6162, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 6162, Parent: 5472, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6165, Parent: 5472)
- sh (PID: 6165, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
- gsd-power (PID: 6165, Parent: 5472, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 7048, Parent: 5472)
- sh (PID: 7048, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
- spice-vdagent (PID: 7048, Parent: 5472, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 7053, Parent: 5472)
- sh (PID: 7053, Parent: 5472, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
- xbrlapi (PID: 7053, Parent: 5472, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q

- gdm3 New Fork (PID: 5414, Parent: 1320)
- Default (PID: 5414, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5415, Parent: 1320)
- Default (PID: 5415, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5425, Parent: 1320)
- Default (PID: 5425, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5431, Parent: 1860)
- pulseaudio (PID: 5431, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gvfsd-fuse New Fork (PID: 5475, Parent: 2038)
- fusermount (PID: 5475, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5497, Parent: 1)
- systemd-user-runtime-dir (PID: 5497, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5604, Parent: 1)
- systemd-localed (PID: 5604, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5892, Parent: 1334)
- pulseaudio (PID: 5892, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5899, Parent: 1)
- geoclue (PID: 5899, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6183, Parent: 1)
- systemd-hostnamed (PID: 6183, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6539, Parent: 1)
- fprintd (PID: 6539, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- systemd New Fork (PID: 6761, Parent: 1)
- systemd-localed (PID: 6761, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed

- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
uwgXkY20gB	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

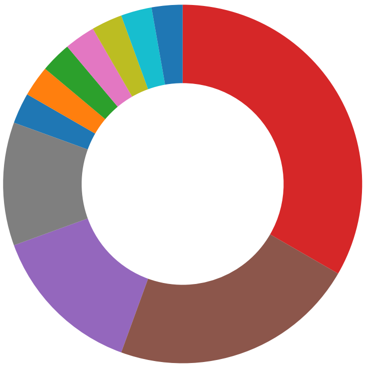
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5251.1.000000002fd88c3b.0000000052a3b712.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5240.1.000000002fd88c3b.0000000052a3b712.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5244.1.000000002fd88c3b.0000000052a3b712.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5248.1.000000002fd88c3b.0000000052a3b712.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5253.1.000000002fd88c3b.0000000052a3b712.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 5 entries				

Jbx Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

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)

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

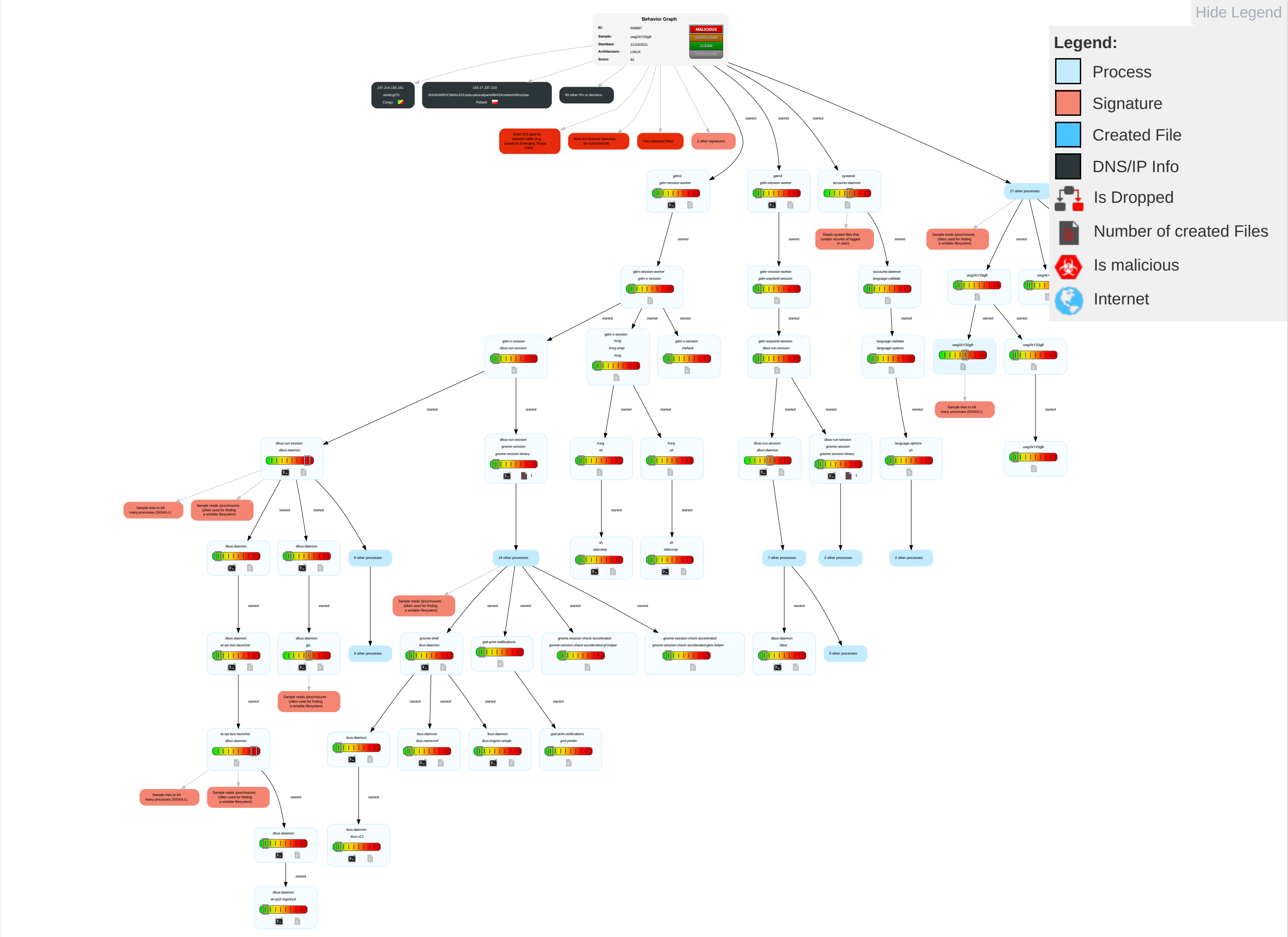
Mitre Att&ck Matrix

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

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
uwgXkY20gB	52%	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
41.57.207.93	unknown	Ghana	🇬🇭	37103	BUSYINTERNETGH	false
219.78.17.104	unknown	Hong Kong	🇭🇰	4760	HKTIMS-APHKTLimitedHK	false
122.80.176.72	unknown	China	🇨🇳	45069	CNNIC-CTTSDNET-APchinatietongShandongnetCN	false
158.50.235.11	unknown	France	🇫🇷	10806	AFP-NETUS	false
197.224.41.168	unknown	Mauritius	🇲🇺	23889	MauritiusTelecomMU	false
32.143.82.87	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
156.3.86.184	unknown	United States	🇺🇸	2920	LACOEUS	false
75.187.158.176	unknown	United States	🇺🇸	10796	TWC-10796-MIDWESTUS	false
218.235.146.193	unknown	Korea Republic of	🇰🇷	9318	SKB-ASSKBroadbandCoLtdKR	false
41.145.154.93	unknown	South Africa	🇿🇦	5713	SAIX-NETZA	false
107.108.1.42	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
197.96.225.141	unknown	South Africa	🇿🇦	3741	ISZA	false
197.159.177.31	unknown	Sao Tome and Principe	🇸🇹	328191	CST-NET-ASST	false
68.250.23.43	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
197.140.232.156	unknown	Algeria	🇩🇿	36891	ICOSNET-ASDZ	false
197.118.32.213	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
197.204.101.52	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
180.205.110.17	unknown	Taiwan; Republic of China (ROC)	🇹🇼	24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
207.104.139.142	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
216.191.44.188	unknown	Canada	🇨🇦	15290	ALLST-15290CA	false
23.137.184.161	unknown	Reserved	?	40098	CASNETUS	false
188.67.250.37	unknown	Finland	🇫🇮	16086	DNAFI	false
98.152.206.154	unknown	United States	🇺🇸	20001	TWC-20001-PACWESTUS	false
158.216.153.182	unknown	Switzerland	🇨🇭	2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
156.51.42.218	unknown	Sweden	🇸🇪	29975	VODACOM-ZA	false
136.215.251.208	unknown	United States	🇺🇸	1585	DNIC-ASBLK-01550-01601US	false
20.64.243.196	unknown	United States	🇺🇸	8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
156.197.234.81	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
41.60.238.109	unknown	Mauritius	🇲🇺	30844	LIQUID-ASGB	false
5.152.105.152	unknown	Georgia	🇬🇪	35805	SILKNET-ASGE	false
196.48.217.167	unknown	Seychelles	🇸🇨	37518	FIBERGRIDSC	false
16.136.106.210	unknown	United States	🇺🇸	unknown	unknown	false
156.46.254.199	unknown	United States	🇺🇸	3527	NIH-NETUS	false
129.178.47.202	unknown	Sweden	🇸🇪	44320	SEBNET-ASSE	false
201.225.63.194	unknown	Panama	🇵🇦	11556	CableWirelessPanamaPA	false
186.167.121.114	unknown	Venezuela	🇻🇪	27717	CorporacionDigitelCAVE	false
94.59.9.110	unknown	United Arab Emirates	🇦🇪	5384	EMIRATES-INTERNETEmiratesInternetAE	false
39.78.11.162	unknown	China	🇨🇳	4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
156.97.115.166	unknown	Chile	🇨🇱	16629	CTCCORPSATELEFONICAEMPRESASCL	false
156.220.29.250	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
94.13.233.250	unknown	United Kingdom	🇬🇧	5607	BSKYB-BROADBAND-ASGB	false
88.30.200.36	unknown	Spain	🇪🇸	3352	TELEFONICA_DE_ESPANAES	false
135.20.62.232	unknown	United States	🇺🇸	18676	AVAYAUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.186.122.47	unknown	Rwanda	🇷🇼	36890	MTNRW-ASNRW	false
197.76.213.128	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
197.240.131.165	unknown	unknown	❓	37705	TOPNETTN	false
156.68.4.51	unknown	United States	🇺🇸	297	AS297US	false
84.118.167.187	unknown	Netherlands	🇳🇱	6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
165.108.36.253	unknown	Japan	🇯🇵	4713	OCNNTTCommunicationsCorporationJP	false
211.158.10.111	unknown	China	🇨🇳	4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
18.245.41.245	unknown	United States	🇺🇸	16509	AMAZON-02US	false
156.10.149.127	unknown	Finland	🇫🇮	39098	BOF-ASFI	false
41.37.208.150	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
41.102.102.210	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
41.94.138.99	unknown	Mozambique	🇲🇿	327700	MoRENetMZ	false
156.149.192.238	unknown	New Zealand	🇳🇿	137	ASGARRConsortiumGARREU	false
139.21.47.133	unknown	Germany	🇩🇪	680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
41.3.151.107	unknown	South Africa	🇿🇦	29975	VODACOM-ZA	false
197.214.155.161	unknown	Congo	🇨🇬	37550	airtelcgCG	false
41.196.116.128	unknown	Egypt	🇪🇬	24863	LINKdotNET-ASEG	false
200.179.139.28	unknown	Brazil	🇧🇷	4230	CLAROSABR	false
119.93.197.79	unknown	Philippines	🇵🇭	9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
41.215.4.18	unknown	Kenya	🇰🇪	15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
185.89.95.61	unknown	Norway	🇳🇴	50531	ABAXNO	false
41.219.191.22	unknown	Nigeria	🇳🇬	30998	NAL-ASNG	false
119.189.161.232	unknown	China	🇨🇳	4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
41.205.252.99	unknown	Sierra Leone	🇸🇱	36928	SIERRATEL-ASSL	false
197.60.107.78	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
156.17.237.210	unknown	Poland	🇵🇱	8970	WASKWROCMAN-EDUeducationalpartofWASKnetworkWroclaw	false
41.95.85.7	unknown	Sudan	🇸🇩	36998	SDN-MOBITELSD	false
202.176.219.164	unknown	Singapore	🇸🇬	9911	CONNECTPLUS-APSingaporeTelecomSG	false
41.145.120.165	unknown	South Africa	🇿🇦	5713	SAIX-NETZA	false
114.8.69.117	unknown	Indonesia	🇮🇩	56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
126.123.117.33	unknown	Japan	🇯🇵	17676	GIGAINFRASoftbankBBCorpJP	false
120.164.66.6	unknown	Indonesia	🇮🇩	4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
197.51.4.241	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
197.204.9.238	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
197.91.228.133	unknown	South Africa	🇿🇦	10474	OPTINETZA	false
156.78.164.220	unknown	United States	🇺🇸	18862	NCS-HEALTHCAREUS	false
41.225.7.170	unknown	Tunisia	🇹🇳	37671	GLOBALNET-ASTN	false
41.149.186.154	unknown	South Africa	🇿🇦	5713	SAIX-NETZA	false
213.177.110.113	unknown	Russian Federation	🇷🇺	12389	ROSTELECOM-ASRU	false
113.128.127.82	unknown	China	🇨🇳	4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
156.231.123.190	unknown	Seychelles	🇸🇨	54600	PEGTECHINCUS	false
41.44.132.66	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
41.96.73.15	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
58.129.125.4	unknown	China	🇨🇳	4847	CNIX-APChinaNetworksInter-ExchangeCN	false
90.163.45.73	unknown	Spain	🇪🇸	12479	UNI2-ASES	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
111.199.204.229	unknown	China	🇨🇳	4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
46.205.93.188	unknown	Poland	🇵🇱	12912	TMPL	false
57.165.126.206	unknown	Belgium	🇧🇪	2686	ATGS-MMD-ASUS	false
209.195.34.71	unknown	United States	🇺🇸	6597	CBDC-6597US	false
138.239.244.108	unknown	Singapore	🇸🇬	8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
37.223.25.195	unknown	Spain	🇪🇸	12430	VODAFONE_ESES	false
173.251.105.100	unknown	United States	🇺🇸	16884	TOURM-3US	false
111.45.52.105	unknown	China	🇨🇳	56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
156.214.15.168	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
87.20.77.126	unknown	Italy	🇮🇹	3269	ASN-IBSNAZIT	false
41.18.99.139	unknown	South Africa	🇿🇦	29975	VODACOM-ZA	false
74.185.53.37	unknown	United States	🇺🇸	6389	BELLSOUTH-NET-BLKUS	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
219.78.17.104	LkypMws5yh	Get hash	malicious	Browse	
197.118.32.213	arm7	Get hash	malicious	Browse	
	yir8ieZzXL	Get hash	malicious	Browse	
	1M4azHIecM	Get hash	malicious	Browse	
197.224.41.168	o4Z7P6CAyR	Get hash	malicious	Browse	
197.204.101.52	vkDtq5ViDc	Get hash	malicious	Browse	
75.187.158.176	x86.light	Get hash	malicious	Browse	
107.108.1.42	hoho.x86	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	arm7	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.132
	FWsCarsq8Q	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	arm	Get hash	malicious	Browse	• 162.213.33.132
	7qvn4qlmi3	Get hash	malicious	Browse	• 162.213.33.132
	JuofJwjQMT	Get hash	malicious	Browse	• 162.213.33.108
	GRPVtMlbK5	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	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
	mYBcqY8XIj	Get hash	malicious	Browse	• 162.213.33.132
	KEgx4lC3Ni	Get hash	malicious	Browse	• 162.213.33.108

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BUSYINTERNETGH	GRPVtMlbK5	Get hash	malicious	Browse	• 41.57.207.98

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	arm7	Get hash	malicious	Browse	• 41.57.232.97
	x86.light	Get hash	malicious	Browse	• 41.57.232.89
	x86	Get hash	malicious	Browse	• 41.57.232.80
	UnHAnaAW.x86	Get hash	malicious	Browse	• 41.57.232.59
	UjdGL7UksU	Get hash	malicious	Browse	• 41.57.207.95
	RaVPWTArgG	Get hash	malicious	Browse	• 41.57.232.84
	uTfW1dzdIk	Get hash	malicious	Browse	• 41.57.207.95
	tI0W00k1vt	Get hash	malicious	Browse	• 41.57.232.49
	arm	Get hash	malicious	Browse	• 41.57.232.59
	EARyrjHCsU	Get hash	malicious	Browse	• 41.57.232.85
	b48zuunBwh	Get hash	malicious	Browse	• 41.57.232.88
	GV2wru9fPr	Get hash	malicious	Browse	• 41.57.232.44
	Imd6cEU2E7	Get hash	malicious	Browse	• 41.57.232.95
	sora.x86	Get hash	malicious	Browse	• 41.57.232.75
	U5q75RGCmQ	Get hash	malicious	Browse	• 41.57.232.59
	apep.mips	Get hash	malicious	Browse	• 41.57.232.59
HKTIMS-APHKTLimitedHK	GzcHogvIYP	Get hash	malicious	Browse	• 1.36.153.234
	HDgtpV43hX	Get hash	malicious	Browse	• 42.98.155.8
	JIUq8a4ITS	Get hash	malicious	Browse	• 42.2.200.149
	9aAl5Mt3Jz	Get hash	malicious	Browse	• 116.48.53.211
	OcO4KUSfwn	Get hash	malicious	Browse	• 42.2.247.189
	PyZcDaysXO	Get hash	malicious	Browse	• 168.70.158.110
	94VG.x86	Get hash	malicious	Browse	• 112.118.154.125
	KKveTTgaAAsecNNaaaa.x86	Get hash	malicious	Browse	• 223.197.228.27
	SYyxBAju45	Get hash	malicious	Browse	• 119.237.195.80
	KG7X7nyxQ4	Get hash	malicious	Browse	• 1.36.117.194
	D0sF4Fm8Za	Get hash	malicious	Browse	• 219.79.161.57
	dAomIYnSHd	Get hash	malicious	Browse	• 1.64.178.117
	6yn3FbemmP	Get hash	malicious	Browse	• 220.246.128.171
	b3astmode.x86	Get hash	malicious	Browse	• 168.70.158.121
	b3astmode.arm7	Get hash	malicious	Browse	• 219.79.185.19
	2hY00mDxD3	Get hash	malicious	Browse	• 112.120.216.137
	soramrk.arm7	Get hash	malicious	Browse	• 42.3.185.104
	2hrxC5NcX5	Get hash	malicious	Browse	• 42.2.229.0
	LkypMws5yh	Get hash	malicious	Browse	• 219.78.17.104
	18vaq1Ah2l	Get hash	malicious	Browse	• 1.36.6.111

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
	7iw4z5I41w	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/5320/oom_score_adj

Process:	/usr/sbin/sshd

/proc/5320/oom_score_adj

File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/proc/5369/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/5372/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/5374/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

/proc/5374/oom_score_adj	
Preview:	0

/proc/5376/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

/proc/5378/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99

/proc/5385/oom_score_adj

Malicious:	false
Preview:	0

/proc/5533/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/5561/oom_score_adj

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

/proc/5564/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/5568/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

/proc/5568/oom_score_adj

SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	0

/proc/5570/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/5572/oom_score_adj

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

/proc/5574/oom_score_adj

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

/proc/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

/proc/5577/oom_score_adj

SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	0

/proc/5884/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/5898/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/6119/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/6182/oom_score_adj

Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA

/proc/6182/oom_score_adj	
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:DXVv:LVv
MD5:	2FF646B97F46BEE3CF5F697BEA7DEA21
SHA1:	77D06106E6BB609A0F4673402681924367AA0361
SHA-256:	D17B23606A994E3B7740F100747960BFBA7BDB814FC38BF0A25B43AFD0A950B9
SHA-512:	2037A816D67E5FBA723304AE91484D0361F1164998C0ECE04BB2B038D1BB76DB2851435C74A6BE33185CB28BF1D61D817D375A21905F33C79C93EE892EB603F3
Malicious:	false
Preview:	5320.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Ej:Ej
MD5:	38C593EFC3531B9C4DABD4214580D922
SHA1:	3F5648CBAF689D3A999C16B5EA40C4E3D28E6698
SHA-256:	C1E0C4E6A4FD1D166871C0C6BB69F52ADB371C2AE71FE6F89C6497EC4E066E97
SHA-512:	8D9D3B87840B2D0E175DB2E70B87551E96F5F25135ACD6DDAF09FD58B6F22BDA509BEBAB5A3E94DDB360685ED500AB64BAB55060239BD43B6459F49741631B 7
Malicious:	false
Preview:	5431.

/run/user/127/ICEauthority	
Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	6.026648813521756
Encrypted:	false
SSDEEP:	12:OxPvK3IwoSveY+vK3aleXxP2o3UNqssXOveY+2o36xP5mhijveY+5tWmxPwWoveG:H/o0qkUofN4ocwqrGodAohPRqVRDC
MD5:	6E27E440F0A2ED212D0CDED0ABA95743
SHA1:	C4A11749B18BE38F10B66F46F79D6F2104E41FBF
SHA-256:	EEB290B58E86B128950A09A5D9E9B03CA99F4A37E7E924A7415080642B1F2C2D
SHA-512:	35916EECE57763F5EE40618BD28C60C4E82E07049350DDDB91C8F4E10AF8A3892CC45A00AA99B4704A65BE024B95FD507283AB81411D2B2993FA4F61DB2AE5A 0
Malicious:	false
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5472..MIT-MAGIC-COOKIE-1..1...b.c..6..H&....XSMP...#local/galassia:@/tmp/.ICE-unix/5472..MIT-MAGIC-COOKIE-1....Rz.......o; {...ICE...!unix/galassia:/tmp/.ICE-unix/5365..MIT-MAGIC-COOKIE-1.....3..O.]....?...ICE...#local/galassia:@/tmp/.ICE-unix/5365..MIT-MAGIC-COOKIE-1...7.#.JB.D0.. R.r...XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.......A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....o.(R...} .9...ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f........E ..c..XSMP...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... ......Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,.:B .o......ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte\|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN... ..N+..$..XSMP...#local/galass

/run/user/127/dconf/user	
Process:	/usr/libexec/gsd-power
File Type:	very short file (no magic)
Category:	dropped

/run/user/127/dconf/user	
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	93B885ADFE0DA089CDF634904FD59F71
SHA1:	5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F
SHA-256:	6E340B9CFFB37A989CA544E6BB780A2C78901D3FB33738768511A30617AFA01D
SHA-512:	B8244D028981D693AF7B456AF8EFA4CAD63D282E19FF14942C246E50D9351D22704A802A71C3580B6370DE4CEB293C324A8423342557D4E5C38438F0E36910EE
Malicious:	false
Preview:	.

/run/user/127/gdm/Xauthority	
Process:	/usr/lib/gdm3/gdm-x-session
File Type:	X11 Xauthority data
Category:	dropped
Size (bytes):	104
Entropy (8bit):	4.920888777625093
Encrypted:	false
SSDEEP:	3:rg/WFllasO93AkTaa9WFllasO93AkTn:rg/WFl2wiaOWFl2win
MD5:	D23A3E79577008872AB8753CE91284D4
SHA1:	25BE72BCE3B732DEC5F1554262F52737A5A6F03E
SHA-256:	5AAE2549A6759824C469B2B39CF0C5B51B94A994A8AE4CC731361462DBC97F47
SHA-512:	E7D6B5A8C0436922940E71F6EF70CA4563AD951924BE9039252B7671C55441397021BFDD7DD6DAD33C4112AE4113BFA6AA6CFF15E7736B4A8A414D9C15CB60C C
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1....`..i..I.e3........galassia....MIT-MAGIC-COOKIE-1....`..i..I.e3....

/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:Imvn:IY
MD5:	7A444EB1194DFB06AB89FC1B5B43F892
SHA1:	99B6D45F9EFF3B801C2FFB5EEC6FADD41E0C4789
SHA-256:	7CB70CE7909646183563673FCDD5244C67572D0A5E18F7BF5C2394B37B727F90
SHA-512:	505D07B0D12A17C9F8718E2B485DD7BE17969E80C3D1D82D293D79EA3FCF7760A253920CB4771E85F0076507DC117E7542BAA67CD85112A92374AD54771EBEB
Malicious:	false
Preview:	5892.

/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:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE00 1
Malicious:	false
Preview:	.mkx.............D......................h.......<.....P.@%.......&......D.......NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta ....Super...Hyper...........evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD 06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB 08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP 3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWN PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181 I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18

/var/cache/motd-news

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

/var/lib/AccountsService/users/gdm.BAWTB1

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

/var/lib/AccountsService/users/gdm.V3BQB1

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

/var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0

Process:	/usr/bin/ibus-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.173424895818757
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWW5WwDNxf19T:q5sU3LWfLUDmQymqSFbfomSLWKxffT
MD5:	5308953354C36ABAAFF7C057738B72DA
SHA1:	9A6BFB48E6749BA204371CF1390553DC30CC5DF3
SHA-256:	961F74AA30210CC2D6041C199C5E8F60CE215B438E412E10F2C2C20BFEB8E91A
SHA-512:	235FECC71B4ADDB9959E68A6D9705E94B683C2B499A2AB17C191871077A6ABD13F3A425AA0D8F3D1A6015BC6D6921117678571E352B90CAD47F1E4A7CF17146
Malicious:	false

/var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0

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-YuSGg8Co,guid=2125a7bd60492d8f8410b4246170cbd2.IBUS_DAEMON_PID=5630.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink

Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	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.L37UB1

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):	5.290767348823813
Encrypted:	false
SSDEEP:	384:7A2gArG+eSzB5Med7dLdFdRdtdbdPdDdHdjdOd9dldidPdJdAdFdcdrdgddhfHd3:k2gqZeSs317uyT8yaqUK+TuYDqtKbjcx
MD5:	43146A89AADB329CB54A925B8DA4C88F
SHA1:	1A60B0A6FF235626CC2376A12416FF67B7F98D64
SHA-256:	5E4C9A51B8FAC08010682EB48B385A387291BBB05C06042FC03293D475FEC7FA

/var/log/Xorg.0.log	
SHA-512:	8CBF7CE24F5D20C06CA5E476412EE8B5DCC96E277E2B7CA73EBD7461DFA978C6295D623F1F5DE42B73F5B952B35C7E2BAD2E9FBCBF3EC9850223A14CC1CEI D2D
Malicious:	false
Preview:	[482.615] (--) Log file renamed from "/var/log/Xorg.pid-5422.log" to "/var/log/Xorg.0.log".[482.640] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[482.649] Build Operating System: linux Ubuntu.[482.655] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[482.663] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[482.679] Build Date: 06 July 2021 10:17:51AM.[482.688] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[482.693] Current version of pixman: 0.38.4.[482.699] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[482.712] 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, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.861289440671699
TrID:	- ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	uwgXkY20gB
File size:	91508
MD5:	949c3108afe02abd57eaae9738d607d3
SHA1:	b0fa61c619dfa80983f98c310fc46b66b5f3d1fb
SHA256:	f620d815094fa7c719cdbbdadee9bfa180ba2940798dcb0d7ebf792124c5ac86
SHA512:	1b3b1e211629d8a065474cab42573c779f867d4a549e3e14d37cf4c7684435189856e04faea15cf468f5bf40bf3da303eae4d879011fab2bb57ee9881b37acb0
SSDEEP:	1536:wPxmkLbgX0FC5+8gCdJyTd4+2XOMOib1PEyCfER+KVaAxwJkaA5hr8:y3bSJYplyTd4eML1PEy3VGkJ5hA
File Content Preview:	.ELF.............*.......@.4....c......4. ...(...............@...@..Z...Z...............`...`B..`B......h..........Q.td...........................././"O.n........#.*@........#.*@. ...o&O.n...l............................../ ./.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	91108
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0x120e0	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x4121c0	0x121c0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4121e4	0x121e4	0x38ac	0x0	0x2	A	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.ctors	PROGBITS	0x426000	0x16000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x426008	0x16008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x426014	0x16014	0x390	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x4263a4	0x163a4	0x6558	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x163a4	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x15a90	0x15a90	4.9026	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x16000	0x426000	0x426000	0x3a4	0x68fc	1.6624	0x6	RW	0x10000		.ctors .dtors .data .bss
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 02:08:09.305010080 CEST	192.168.2.23	1.1.1.1	0xaa9e	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Oct 21, 2021 02:08:09.305109024 CEST	192.168.2.23	1.1.1.1	0xa7d8	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Oct 21, 2021 02:08:09.426495075 CEST	192.168.2.23	1.1.1.1	0xd72b	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 02:08:09.322051048 CEST	1.1.1.1	192.168.2.23	0xaa9e	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Oct 21, 2021 02:08:09.322051048 CEST	1.1.1.1	192.168.2.23	0xaa9e	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: uwgXkY20gB PID: 5237 Parent PID: 5111

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	/tmp/uwgXkY20gB
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: uwgXkY20gB PID: 5239 Parent PID: 5237

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5240 Parent PID: 5237

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5241 Parent PID: 5237

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5243 Parent PID: 5237

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5244 Parent PID: 5237

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5248 Parent PID: 5237

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5251 Parent PID: 5248

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: uwgXkY20gB PID: 5253 Parent PID: 5248

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uwgXkY20gB PID: 5255 Parent PID: 5253

General

Start time:	02:07:24
Start date:	21/10/2021
Path:	/tmp/uwgXkY20gB
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: dash PID: 5275 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5275 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.f7vJ3oarTQ
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5276 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5276 Parent PID: 4331

General

Start time:	02:08:06
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: 5277 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash

Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5277 Parent PID: 4331

General

Start time:	02:08:06
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: 5278 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5278 Parent PID: 4331

General

Start time:	02:08:06
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: 5279 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5279 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.f7vJ3oarTQ
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5280 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5280 Parent PID: 4331

General

Start time:	02:08:06
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: 5281 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5281 Parent PID: 4331

General

Start time:	02:08:06
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: 5282 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5282 Parent PID: 4331

General

Start time:	02:08:06
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: 5285 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5285 Parent PID: 4331

General

Start time:	02:08:06
Start date:	21/10/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.f7vJ3oarTQ /tmp/tmp.mQ9Xgt5KVB /tmp/tmp.SEXT8WVCCo
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: systemd PID: 5304 Parent PID: 1

General

Start time:	02:08:08
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5304 Parent PID: 1

General

Start time:	02:08:08
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: 5315 Parent PID: 1

General

Start time:	02:08:12
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5315 Parent PID: 1

General

Start time:	02:08:12
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: 5320 Parent PID: 1

General

Start time:	02:08:12
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:	02:08:12
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: gdm3 PID: 5323 Parent PID: 1320

General

Start time:	02:08:19
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5323 Parent PID: 1320

General

Start time:	02:08:19
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: 5326 Parent PID: 1320

General

Start time:	02:08:19
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5326 Parent PID: 1320

General

Start time:	02:08:19
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: 5327 Parent PID: 1

General

Start time:	02:08:19
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: 5327 Parent PID: 1

General

Start time:	02:08:19
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: 5349 Parent PID: 5327

General

Start time:	02:08:20
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: 5349 Parent PID: 5327

General

Start time:	02:08:20
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: 5350 Parent PID: 5349

General

Start time:	02:08:20
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: 5350 Parent PID: 5349

General

Start time:	02:08:20
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: 5351 Parent PID: 5350

General

Start time:	02:08:20
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: 5351 Parent PID: 5350

General

Start time:	02:08:20
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: 5352 Parent PID: 5351

General

Start time:	02:08:20
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5352 Parent PID: 5351

General

Start time:	02:08:20
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: 5353 Parent PID: 5351

General

Start time:	02:08:20
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5353 Parent PID: 5351

General

Start time:	02:08:20
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: 5356 Parent PID: 1320

General

Start time:	02:08:21
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: 5356 Parent PID: 1320

General

Start time:	02:08:21
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: 5360 Parent PID: 5356

General

Start time:	02:08:23
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: 5360 Parent PID: 5356

General

Start time:	02:08:23

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: 5363 Parent PID: 5360

General

Start time:	02:08:23
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: 5363 Parent PID: 5360

General

Start time:	02:08:23
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: 5364 Parent PID: 5363

General

Start time:	02:08:23
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: 5364 Parent PID: 5363

General

Start time:	02:08:23
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: 5368 Parent PID: 5364

General

Start time:	02:08:24
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: 5369 Parent PID: 5368

General

Start time:	02:08:24
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: 5369 Parent PID: 5368

General

Start time:	02:08:24
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: 5371 Parent PID: 5364

General

Start time:	02:08:24
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: 5372 Parent PID: 5371

General

Start time:	02:08:24
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: 5372 Parent PID: 5371

General

Start time:	02:08:24
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: 5373 Parent PID: 5364

General

Start time:	02:08:24
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: 5374 Parent PID: 5373

General

Start time:	02:08:24
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: 5374 Parent PID: 5373

General

Start time:	02:08:24
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: 5375 Parent PID: 5364

General

Start time:	02:08:25
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: 5376 Parent PID: 5375

General

Start time:	02:08:25
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: 5376 Parent PID: 5375

General

Start time:	02:08:25
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: 5377 Parent PID: 5364

General

Start time:	02:08:25
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: 5378 Parent PID: 5377

General

Start time:	02:08:25
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: 5378 Parent PID: 5377

General

Start time:	02:08:25
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: 5379 Parent PID: 5364

General

Start time:	02:08:26
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:	02:08:26
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:	02:08:26
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: 5364

General

Start time:	02:08:26
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:	02:08:26
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:	02:08:26
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: 5365 Parent PID: 5363

General

Start time:	02:08:23
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: 5365 Parent PID: 5363

General

Start time:	02:08:23
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: 5365 Parent PID: 5363

General

Start time:	02:08:23
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: 5386 Parent PID: 5365

General

Start time:	02:08:27
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: 5386 Parent PID: 5365

General

Start time:	02:08:27
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: 5387 Parent PID: 5365

General

Start time:	02:08:27
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: 5387 Parent PID: 5365

General

Start time:	02:08:27
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: 5387 Parent PID: 5365

General

Start time:	02:08:28
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: 5413 Parent PID: 1320

General

Start time:	02:08:31
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: 5413 Parent PID: 1320

General

Start time:	02:08:31
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: 5420 Parent PID: 5413

General

Start time:	02:08:33
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: 5420 Parent PID: 5413

General

Start time:	02:08:33
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: 5422 Parent PID: 5420

General

Start time:	02:08:34
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: 5422 Parent PID: 5420

General

Start time:	02:08:34
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: 5422 Parent PID: 5420

General

Start time:	02:08:34
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: 5422 Parent PID: 5420

General

Start time:	02:08:34
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: 5460 Parent PID: 5422

General

Start time:	02:08:46
Start date:	21/10/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5460 Parent PID: 5422

General

Start time:	02:08:46
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: 5461 Parent PID: 5460

General

Start time:	02:08:46
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5461 Parent PID: 5460

General

Start time:	02:08:46
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: 5887 Parent PID: 5422

General

Start time:	02:09:23
Start date:	21/10/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5887 Parent PID: 5422

General

Start time:	02:09:24
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: 5888 Parent PID: 5887

General

Start time:	02:09:24
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5888 Parent PID: 5887

General

General

Start time:	02:09:24
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: 5469 Parent PID: 5420

General

Start time:	02:08:52
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: 5469 Parent PID: 5420

General

Start time:	02:08:52
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: 5470 Parent PID: 5420

General

Start time:	02:08:52
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: 5470 Parent PID: 5420

General

Start time:	02:08:52
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: 5471 Parent PID: 5470

General

Start time:	02:08:52
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: 5471 Parent PID: 5470

General

Start time:	02:08:52
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: 5532 Parent PID: 5471

General

Start time:	02:09:02
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: 5533 Parent PID: 5532

General

Start time:	02:09:02
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: 5533 Parent PID: 5532

General

Start time:	02:09:02
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: 5538 Parent PID: 5533

General

Start time:	02:09:02
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: 5538 Parent PID: 5533

General

Start time:	02:09:02
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: 5897 Parent PID: 5538

General

Start time:	02:09:26
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: 5898 Parent PID: 5897

General

Start time:	02:09:26
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: 5898 Parent PID: 5897

General

Start time:	02:09:27
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: 5560 Parent PID: 5471

General

Start time:	02:09:05
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: 5561 Parent PID: 5560

General

Start time:	02:09:05
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: 5561 Parent PID: 5560

General

Start time:	02:09:05
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: 5563 Parent PID: 5471

General

Start time:	02:09:05
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: 5564 Parent PID: 5563

General

Start time:	02:09:05
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: 5564 Parent PID: 5563

General

Start time:	02:09:06
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: 5567 Parent PID: 5471

General

Start time:	02:09:06
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: 5568 Parent PID: 5567

General

Start time:	02:09:06
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: 5568 Parent PID: 5567

General

Start time:	02:09:06
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: 5569 Parent PID: 5471

General

Start time:	02:09:06
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: 5570 Parent PID: 5569

General

Start time:	02:09:06
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: 5570 Parent PID: 5569

General

Start time:	02:09:06
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: 5571 Parent PID: 5471

General

Start time:	02:09:06
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: 5572 Parent PID: 5571

General

Start time:	02:09:06
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: 5572 Parent PID: 5571

General

Start time:	02:09:06
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: 5573 Parent PID: 5471

General

Start time:	02:09:06

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:	02:09:06
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:	02:09:06
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: 5471

General

Start time:	02:09:07
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:	02:09:07
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:	02:09:07
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: 5883 Parent PID: 5471

General

Start time:	02:09:23
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: 5884 Parent PID: 5883

General

Start time:	02:09:23
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: 5884 Parent PID: 5883

General

Start time:	02:09:23
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: 6118 Parent PID: 5471

General

Start time:	02:09:28
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: 6119 Parent PID: 6118

General

Start time:	02:09:28
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: 6119 Parent PID: 6118

General

Start time:	02:09:28
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: 6181 Parent PID: 5471

General

Start time:	02:09:43
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: 6182 Parent PID: 6181

General

Start time:	02:09:43
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: 6182 Parent PID: 6181

General

Start time:	02:09:43
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: 5472 Parent PID: 5470

General

Start time:	02:08:52
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: 5472 Parent PID: 5470

General

Start time:	02:08:52
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: 5472 Parent PID: 5470

General

Start time:	02:08:52
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: 5473 Parent PID: 5472

General

Start time:	02:08:53
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: gnome-session-check-accelerated PID: 5473 Parent PID: 5472

General

Start time:	02:08:53
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: 5539 Parent PID: 5473

General

Start time:	02:09:03
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: 5539 Parent PID: 5473

General

Start time:	02:09:03
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: 5549 Parent PID: 5473

General

Start time:	02:09:04
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: 5549 Parent PID: 5473

General

Start time:	02:09:04
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: 5578 Parent PID: 5472

General

Start time:	02:09:07
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: 5578 Parent PID: 5472

General

Start time:	02:09:07
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: 5579 Parent PID: 5472

General

Start time:	02:09:08
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: 5579 Parent PID: 5472

General

Start time:	02:09:08
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: 5579 Parent PID: 5472

General

Start time:	02:09:08
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: 5630 Parent PID: 5579

General

Start time:	02:09:21
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: 5630 Parent PID: 5579

General

Start time:	02:09:21
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: 5879 Parent PID: 5630

General

Start time:	02:09:22
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: 5879 Parent PID: 5630

General

Start time:	02:09:22
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: 5881 Parent PID: 5630

General

Start time:	02:09:22
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: 5882 Parent PID: 5881

General

Start time:	02:09:22
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: 5882 Parent PID: 1

General

Start time:	02:09:22
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: 6154 Parent PID: 5630

General

Start time:	02:09:37
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: 6154 Parent PID: 5630

General

Start time:	02:09:37
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: 6136 Parent PID: 5472

General

Start time:	02:09:33
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: 6136 Parent PID: 5472

General

Start time:	02:09:33
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: 6136 Parent PID: 5472

General

Start time:	02:09:33
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: 6138 Parent PID: 5472

General

Start time:	02:09:33
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: 6138 Parent PID: 5472

General

Start time:	02:09:33
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: 6138 Parent PID: 5472

General

Start time:	02:09:33
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: 6140 Parent PID: 5472

General

Start time:	02:09:33
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: 6140 Parent PID: 5472

General

Start time:	02:09:33
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: 6140 Parent PID: 5472

General

Start time:	02:09:34
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: 6141 Parent PID: 5472

General

Start time:	02:09:33
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: 5472

General

Start time:	02:09:34
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: 6141 Parent PID: 5472

General

Start time:	02:09:34
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: 6142 Parent PID: 5472

General

Start time:	02:09:34
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: 6142 Parent PID: 5472

General

Start time:	02:09:34
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: 6142 Parent PID: 5472

General

Start time:	02:09:34
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: 6462 Parent PID: 6142

General

Start time:	02:09:47
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: 6463 Parent PID: 6462

General

Start time:	02:09:47
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: 6463 Parent PID: 1

General

Start time:	02:09:47
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: 6143 Parent PID: 5472

General

Start time:	02:09:34
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: 5472

General

Start time:	02:09:35
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: 6143 Parent PID: 5472

General

Start time:	02:09:35
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: 6145 Parent PID: 5472

General

Start time:	02:09:35
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: 5472

General

Start time:	02:09:35
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: 6145 Parent PID: 5472

General

Start time:	02:09:35
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: 6146 Parent PID: 5472

General

Start time:	02:09:35
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: 5472

General

Start time:	02:09:35
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: 6146 Parent PID: 5472

General

Start time:	02:09:36
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: 6149 Parent PID: 5472

General

Start time:	02:09:36
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: sh PID: 6149 Parent PID: 5472

General

Start time:	02:09:36
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: 6149 Parent PID: 5472

General

Start time:	02:09:37
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: 6153 Parent PID: 5472

General

Start time:	02:09:36
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: sh PID: 6153 Parent PID: 5472

General

Start time:	02:09:37
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: 6153 Parent PID: 5472

General

Start time:	02:09:37
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: 6156 Parent PID: 5472

General

Start time:	02:09:37
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: 5472

General

Start time:	02:09:37
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: 6156 Parent PID: 5472

General

Start time:	02:09:38
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: 6157 Parent PID: 5472

General

Start time:	02:09:38
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: 6157 Parent PID: 5472

General

Start time:	02:09:38
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: 6157 Parent PID: 5472

General

Start time:	02:09:39
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: 6162 Parent PID: 5472

General

Start time:	02:09:39
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: 6162 Parent PID: 5472

General

Start time:	02:09:39
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: 6162 Parent PID: 5472

General

Start time:	02:09:40
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: 6165 Parent PID: 5472

General

Start time:	02:09:39
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: 6165 Parent PID: 5472

General

Start time:	02:09:40
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: 6165 Parent PID: 5472

General

Start time:	02:09:40
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: 7048 Parent PID: 5472

General

Start time:	02:10:10
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: 7048 Parent PID: 5472

General

Start time:	02:10:10
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: 7048 Parent PID: 5472

General

Start time:	02:10:11
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: 7053 Parent PID: 5472

General

Start time:	02:10:13
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: 7053 Parent PID: 5472

General

Start time:	02:10:13
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: 7053 Parent PID: 5472

General

Start time:	02:10:14
Start date:	21/10/2021
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5414 Parent PID: 1320

General

Start time:	02:08:31
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5414 Parent PID: 1320

General

Start time:	02:08:31
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: 5415 Parent PID: 1320

General

Start time:	02:08:31
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5415 Parent PID: 1320

General

Start time:	02:08:31
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: 5425 Parent PID: 1320

General

Start time:	02:08:37
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5425 Parent PID: 1320

General

Start time:	02:08:37
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: 5431 Parent PID: 1860

General

Start time:	02:08:42
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5431 Parent PID: 1860

General

Start time:	02:08:42
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: 5475 Parent PID: 2038

General

Start time:	02:08:55
Start date:	21/10/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5475 Parent PID: 2038

General

Start time:	02:08:55
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: 5497 Parent PID: 1

General

Start time:	02:08:57
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: 5497 Parent PID: 1

General

Start time:	02:08:57
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: 5604 Parent PID: 1

General

Start time:	02:09:22
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: 5604 Parent PID: 1

General

Start time:	02:09:22
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: 5892 Parent PID: 1334

General

Start time:	02:09:26
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd

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

Analysis Process: pulseaudio PID: 5892 Parent PID: 1334

General

Start time:	02:09:26
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: 5899 Parent PID: 1

General

Start time:	02:09:27
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5899 Parent PID: 1

General

Start time:	02:09:27
Start date:	21/10/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 6183 Parent PID: 1

General

Start time:	02:09:44
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: 6183 Parent PID: 1

General

Start time:	02:09:44

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: 6539 Parent PID: 1

General

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

Analysis Process: fprintd PID: 6539 Parent PID: 1

General

Start time:	02:10:03
Start date:	21/10/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84

Analysis Process: systemd PID: 6761 Parent PID: 1

General

Start time:	02:10:04
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: 6761 Parent PID: 1

General

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