JOE Sandbox Cloud BASIC

ID: 506681
Sample Name: arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:52:46
Date: 21/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Linux Analysis Report arm

Overview

General Information

Sample Name:	arm
Analysis ID:	506681
MD5:	b03983514a53cfd.
SHA1:	77a0aeccab5317..
SHA256:	171e2181f456498.
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

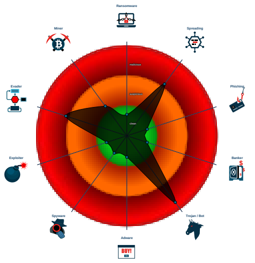
Mirai

Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

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

Classification



Analysis Advice

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

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	506681
Start date:	21.10.2021
Start time:	01:52:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arm
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal96.spre.troj.evad.lin@0/104@3/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 5213, Parent: 1)
- logrotate (PID: 5213, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5311, Parent: 5213)
  - gzip (PID: 5311, Parent: 5213, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5312, Parent: 5213)
  - sh (PID: 5312, Parent: 5213, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
    - sh New Fork (PID: 5313, Parent: 5312)
    - invoke-rc.d (PID: 5313, Parent: 5312, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart

      - invoke-rc.d New Fork (PID: 5314, Parent: 5313)
      - runlevel (PID: 5314, Parent: 5313, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5315, Parent: 5313)
      - systemctl (PID: 5315, Parent: 5313, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5320, Parent: 5313)
      - ls (PID: 5320, Parent: 5313, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5321, Parent: 5313)
      - systemctl (PID: 5321, Parent: 5313, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 5322, Parent: 5213)
  - gzip (PID: 5322, Parent: 5213, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5323, Parent: 5213)
  - sh (PID: 5323, Parent: 5213, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
    - sh New Fork (PID: 5324, Parent: 5323)
    - rsyslog-rotate (PID: 5324, Parent: 5323, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
      - rsyslog-rotate New Fork (PID: 5325, Parent: 5324)
      - systemctl (PID: 5325, Parent: 5324, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5218, Parent: 1)
- install (PID: 5218, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5297, Parent: 1)
- find (PID: 5297, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5316, Parent: 1)
- mandb (PID: 5316, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- arm (PID: 5339, Parent: 5121, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm
  - arm New Fork (PID: 5341, Parent: 5339)
  - arm New Fork (PID: 5342, Parent: 5339)
  - arm New Fork (PID: 5344, Parent: 5339)
  - arm New Fork (PID: 5345, Parent: 5339)
  - arm New Fork (PID: 5348, Parent: 5339)
  - arm New Fork (PID: 5352, Parent: 5339)
    - arm New Fork (PID: 5355, Parent: 5352)
    - arm New Fork (PID: 5357, Parent: 5352)
      - arm New Fork (PID: 5359, Parent: 5357)
- systemd New Fork (PID: 5402, Parent: 1)
- whoopsie (PID: 5402, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5425, Parent: 1)
- sshd (PID: 5425, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5426, Parent: 1)
- sshd (PID: 5426, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5429, Parent: 1320)
- Default (PID: 5429, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5434, Parent: 1320)
- Default (PID: 5434, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5435, Parent: 1)
- accounts-daemon (PID: 5435, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5452, Parent: 5435)
  - language-validate (PID: 5452, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5453, Parent: 5452)
    - language-options (PID: 5453, Parent: 5452, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5454, Parent: 5453)
      - sh (PID: 5454, Parent: 5453, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5455, Parent: 5454)
        - locale (PID: 5455, Parent: 5454, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5456, Parent: 5454)
        - grep (PID: 5456, Parent: 5454, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm3 New Fork (PID: 5457, Parent: 1320)
- gdm-session-worker (PID: 5457, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5461, Parent: 5457)
  - gdm-wayland-session (PID: 5461, Parent: 5457, 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: 5464, Parent: 5461)
    - dbus-run-session (PID: 5464, Parent: 5461, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
      - dbus-run-session New Fork (PID: 5465, Parent: 5464)
      - dbus-daemon (PID: 5465, Parent: 5464, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5471, Parent: 5465)
          - dbus-daemon New Fork (PID: 5472, Parent: 5471)
          - false (PID: 5472, Parent: 5471, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5474, Parent: 5465)
          - dbus-daemon New Fork (PID: 5475, Parent: 5474)
          - false (PID: 5475, Parent: 5474, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5476, Parent: 5465)
          - dbus-daemon New Fork (PID: 5477, Parent: 5476)
          - false (PID: 5477, Parent: 5476, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5478, Parent: 5465)
          - dbus-daemon New Fork (PID: 5479, Parent: 5478)
          - false (PID: 5479, Parent: 5478, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5480, Parent: 5465)
          - dbus-daemon New Fork (PID: 5481, Parent: 5480)
          - false (PID: 5481, Parent: 5480, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5482, Parent: 5465)
          - dbus-daemon New Fork (PID: 5483, Parent: 5482)
          - false (PID: 5483, Parent: 5482, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5485, Parent: 5465)
          - dbus-daemon New Fork (PID: 5486, Parent: 5485)
          - false (PID: 5486, Parent: 5485, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - dbus-run-session New Fork (PID: 5466, Parent: 5464)
      - gnome-session (PID: 5466, Parent: 5464, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
      - gnome-session-binary (PID: 5466, Parent: 5464, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary New Fork (PID: 5487, Parent: 5466)

        - session-migration (PID: 5487, Parent: 5466, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
        - gnome-session-binary New Fork (PID: 5488, Parent: 5466)
        - sh (PID: 5488, Parent: 5466, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
        - gnome-shell (PID: 5488, Parent: 5466, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5496, Parent: 1320)
- gdm-session-worker (PID: 5496, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5523, Parent: 5496)
  - gdm-x-session (PID: 5523, Parent: 5496, 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: 5525, Parent: 5523)
    - Xorg (PID: 5525, Parent: 5523, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg.wrap (PID: 5525, Parent: 5523, 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: 5525, Parent: 5523, 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: 5553, Parent: 5525)
      - sh (PID: 5553, Parent: 5525, 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: 5554, Parent: 5553)
        - xkbcomp (PID: 5554, Parent: 5553, 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: 5986, Parent: 5525)
      - sh (PID: 5986, Parent: 5525, 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: 5987, Parent: 5986)
        - xkbcomp (PID: 5987, Parent: 5986, 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: 5567, Parent: 5523)
    - Default (PID: 5567, Parent: 5523, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
    - gdm-x-session New Fork (PID: 5568, Parent: 5523)
    - dbus-run-session (PID: 5568, Parent: 5523, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
      - dbus-run-session New Fork (PID: 5569, Parent: 5568)
      - dbus-daemon (PID: 5569, Parent: 5568, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5631, Parent: 5569)
          - dbus-daemon New Fork (PID: 5632, Parent: 5631)
          - at-spi-bus-launcher (PID: 5632, Parent: 5631, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
            - at-spi-bus-launcher New Fork (PID: 5637, Parent: 5632)
            - dbus-daemon (PID: 5637, Parent: 5632, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
              - dbus-daemon New Fork (PID: 5994, Parent: 5637)
                - dbus-daemon New Fork (PID: 5995, Parent: 5994)
                - at-spi2-registryd (PID: 5995, Parent: 5994, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
        - dbus-daemon New Fork (PID: 5661, Parent: 5569)
          - dbus-daemon New Fork (PID: 5662, Parent: 5661)
          - false (PID: 5662, Parent: 5661, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5664, Parent: 5569)
          - dbus-daemon New Fork (PID: 5665, Parent: 5664)
          - false (PID: 5665, Parent: 5664, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5666, Parent: 5569)
          - dbus-daemon New Fork (PID: 5667, Parent: 5666)
          - false (PID: 5667, Parent: 5666, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5668, Parent: 5569)
          - dbus-daemon New Fork (PID: 5669, Parent: 5668)
          - false (PID: 5669, Parent: 5668, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5670, Parent: 5569)
          - dbus-daemon New Fork (PID: 5671, Parent: 5670)
          - false (PID: 5671, Parent: 5670, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5672, Parent: 5569)
          - dbus-daemon New Fork (PID: 5673, Parent: 5672)
          - false (PID: 5673, Parent: 5672, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5675, Parent: 5569)
          - dbus-daemon New Fork (PID: 5676, Parent: 5675)
          - false (PID: 5676, Parent: 5675, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5979, Parent: 5569)
          - dbus-daemon New Fork (PID: 5980, Parent: 5979)
          - ibus-portal (PID: 5980, Parent: 5979, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
        - dbus-daemon New Fork (PID: 6207, Parent: 5569)
          - dbus-daemon New Fork (PID: 6208, Parent: 6207)
          - gjs (PID: 6208, Parent: 6207, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
        - dbus-daemon New Fork (PID: 6276, Parent: 5569)
          - dbus-daemon New Fork (PID: 6277, Parent: 6276)
          - false (PID: 6277, Parent: 6276, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - dbus-run-session New Fork (PID: 5570, Parent: 5568)
      - gnome-session (PID: 5570, Parent: 5568, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
      - gnome-session-binary (PID: 5570, Parent: 5568, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary New Fork (PID: 5571, Parent: 5570)
        - gnome-session-check-accelerated (PID: 5571, Parent: 5570, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
          - gnome-session-check-accelerated New Fork (PID: 5638, Parent: 5571)
          - gnome-session-check-accelerated-gl-helper (PID: 5638, Parent: 5571, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
          - gnome-session-check-accelerated New Fork (PID: 5648, Parent: 5571)
          - gnome-session-check-accelerated-gles-helper (PID: 5648, Parent: 5571, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
        - gnome-session-binary New Fork (PID: 5677, Parent: 5570)
        - session-migration (PID: 5677, Parent: 5570, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration

- gnome-session-binary New Fork (PID: 5678, Parent: 5570)
- sh (PID: 5678, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
- gnome-shell (PID: 5678, Parent: 5570, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
  - gnome-shell New Fork (PID: 5784, Parent: 5678)
  - ibus-daemon (PID: 5784, Parent: 5678, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
    - ibus-daemon New Fork (PID: 5908, Parent: 5784)
    - ibus-memconf (PID: 5908, Parent: 5784, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
    - ibus-daemon New Fork (PID: 5939, Parent: 5784)
      - ibus-daemon New Fork (PID: 5942, Parent: 5939)
      - ibus-x11 (PID: 5942, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
    - ibus-daemon New Fork (PID: 6251, Parent: 5784)
    - ibus-engine-simple (PID: 6251, Parent: 5784, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
- gnome-session-binary New Fork (PID: 6228, Parent: 5570)
- sh (PID: 6228, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
- gsd-sharing (PID: 6228, Parent: 5570, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
- gnome-session-binary New Fork (PID: 6230, Parent: 5570)
- sh (PID: 6230, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
- gsd-wacom (PID: 6230, Parent: 5570, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 6232, Parent: 5570)
- sh (PID: 6232, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
- gsd-color (PID: 6232, Parent: 5570, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 6233, Parent: 5570)
- sh (PID: 6233, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
- gsd-keyboard (PID: 6233, Parent: 5570, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 6234, Parent: 5570)
- sh (PID: 6234, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
- gsd-print-notifications (PID: 6234, Parent: 5570, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
  - gsd-print-notifications New Fork (PID: 6554, Parent: 6234)
    - gsd-print-notifications New Fork (PID: 6555, Parent: 6554)
    - gsd-printer (PID: 6555, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 6235, Parent: 5570)
- sh (PID: 6235, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
- gsd-rfkill (PID: 6235, Parent: 5570, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6236, Parent: 5570)
- sh (PID: 6236, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
- gsd-smartcard (PID: 6236, Parent: 5570, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6238, Parent: 5570)
- sh (PID: 6238, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
- gsd-datetime (PID: 6238, Parent: 5570, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6239, Parent: 5570)
- sh (PID: 6239, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
- gsd-media-keys (PID: 6239, Parent: 5570, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6240, Parent: 5570)
- sh (PID: 6240, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
- gsd-screensaver-proxy (PID: 6240, Parent: 5570, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6241, Parent: 5570)
- sh (PID: 6241, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
- gsd-sound (PID: 6241, Parent: 5570, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6248, Parent: 5570)
- sh (PID: 6248, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
- gsd-a11y-settings (PID: 6248, Parent: 5570, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6249, Parent: 5570)
- sh (PID: 6249, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 6249, Parent: 5570, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6254, Parent: 5570)
- sh (PID: 6254, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
- gsd-power (PID: 6254, Parent: 5570, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 7121, Parent: 5570)
- sh (PID: 7121, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
- spice-vdagent (PID: 7121, Parent: 5570, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 7125, Parent: 5570)
- sh (PID: 7125, Parent: 5570, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
- xbrlapi (PID: 7125, Parent: 5570, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q

- gdm3 New Fork (PID: 5513, Parent: 1320)
- Default (PID: 5513, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5518, Parent: 1320)
- Default (PID: 5518, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5528, Parent: 1320)
- Default (PID: 5528, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5533, Parent: 1860)
- pulseaudio (PID: 5533, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gvfsd-fuse New Fork (PID: 5572, Parent: 2038)
- fusermount (PID: 5572, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs

- systemd New Fork (PID: 5595, Parent: 1)
  - systemd-user-runtime-dir (PID: 5595, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5703, Parent: 1)
  - systemd-localed (PID: 5703, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5991, Parent: 1334)
  - pulseaudio (PID: 5991, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5996, Parent: 1)
  - geoclue (PID: 5996, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6278, Parent: 1)
  - systemd-hostnamed (PID: 6278, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6652, Parent: 1)
  - systemd-localed (PID: 6652, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 6684, Parent: 1)
  - fprintd (PID: 6684, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
arm	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	0xa3f8:$s1: PROT_EXEC\|PROT_WRITE failed. 0xa467:$s2: $Id: UPX 0xa418:$s3: $Info: This file is packed with the UPX executable packer

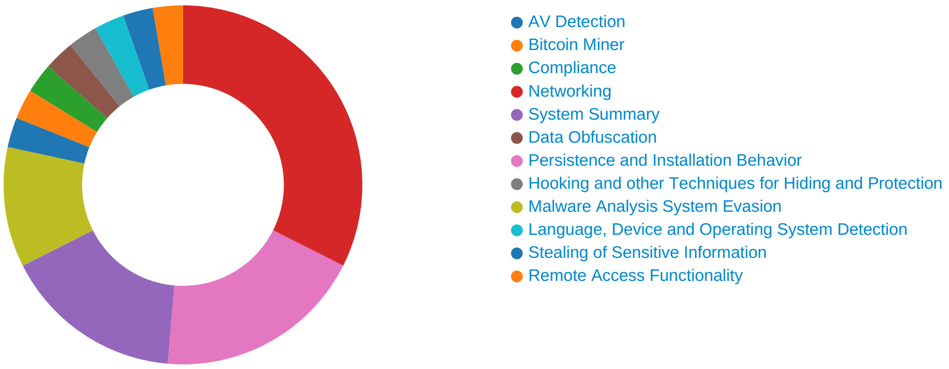
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5355.1.000000008d936394.000000000e200f3a.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5344.1.000000008d936394.000000000e200f3a.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5359.1.000000008d936394.000000000e200f3a.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5348.1.000000008d936394.000000000e200f3a.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5352.1.000000008d936394.000000000e200f3a.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 5 entries				

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

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

Uses known network protocols on non-standard ports

System Summary:

Sample tries to kill many processes (SIGKILL)

Data Obfuscation:

Sample is packed with UPX

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

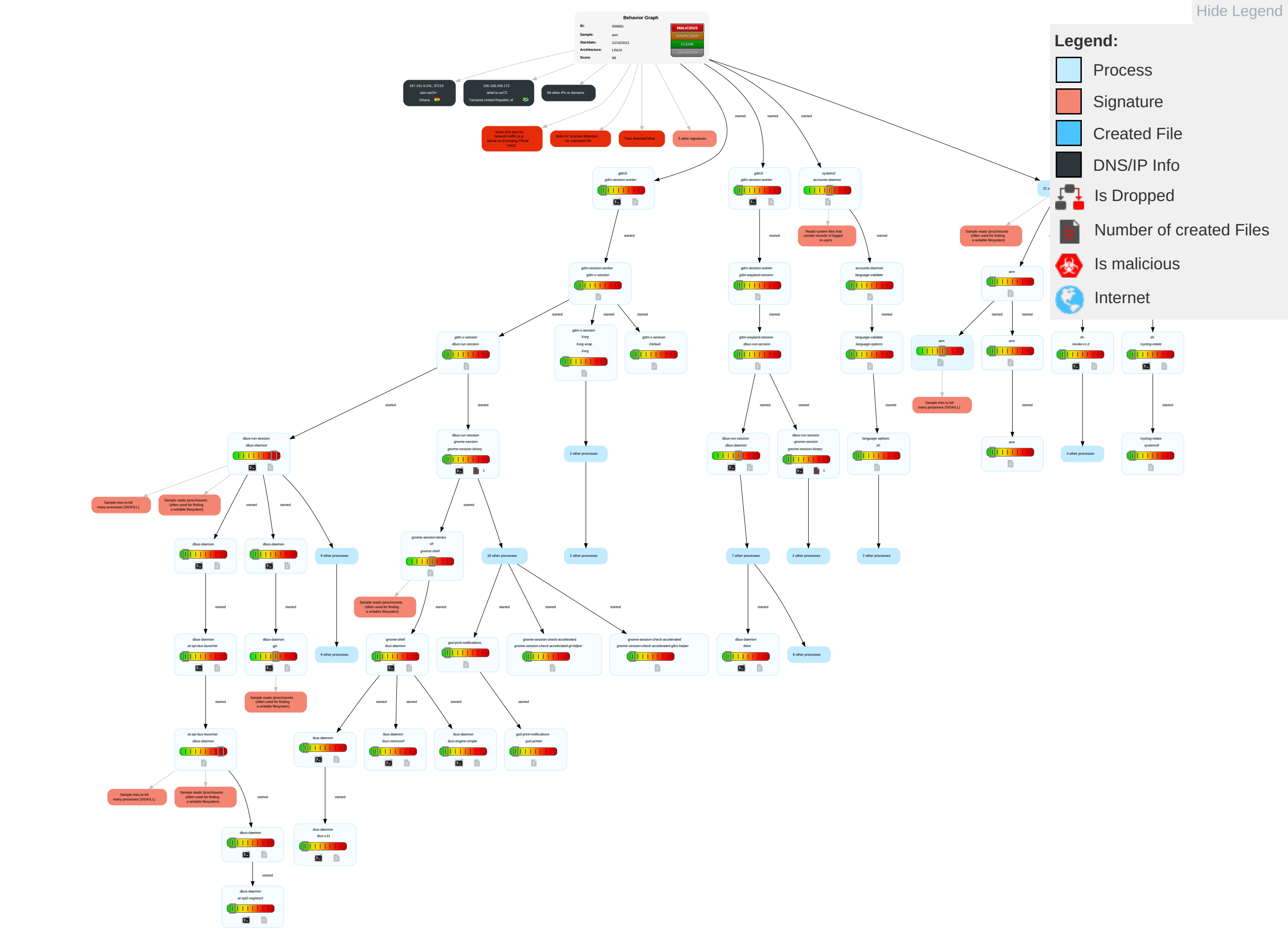
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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)	Obfuscated Files or Information 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Indicator Removal on Host 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipu App Sto Rankin or Ratin

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arm	23%	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	

Source	Detection	Scanner	Label	Link
http://feedback.redkolibri.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.33.132	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.127.73.180	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
197.47.156.113	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
116.123.188.31	unknown	Korea Republic of	🇰🇷	9318	SKB-ASSKBroadbandCoLtdKR	false
41.215.4.49	unknown	Kenya	🇰🇪	15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
197.86.54.124	unknown	South Africa	🇿🇦	10474	OPTINETZA	false
67.214.165.244	unknown	United States	🇺🇸	12260	CUSTOMDOTNETUS	false
197.141.7.49	unknown	Algeria	🇩🇿	36891	ICOSNET-ASDZ	false
156.193.80.170	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
98.150.50.118	unknown	United States	🇺🇸	20001	TWC-20001-PACWESTUS	false
41.14.214.62	unknown	South Africa	🇿🇦	29975	VODACOM-ZA	false
212.175.254.52	unknown	Turkey	🇹🇷	9121	TTNETTR	false
197.60.132.56	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
156.133.239.102	unknown	Luxembourg	🇱🇺	29975	VODACOM-ZA	false
220.58.199.84	unknown	Japan	🇯🇵	17676	GIGAINFRASoftbankBBCorpJP	false
34.53.140.87	unknown	United States	🇺🇸	2686	ATGS-MMD-ASUS	false
5.172.117.173	unknown	Italy	🇮🇹	28890	INSYS-ASINSYSISPRU	false
156.174.55.165	unknown	Egypt	🇪🇬	36992	ETISALAT-MISREG	false
208.61.249.200	unknown	United States	🇺🇸	6389	BELLSOUTH-NET-BLKUS	false
41.68.96.125	unknown	Egypt	🇪🇬	24835	RAYA-ASEG	false
210.136.146.227	unknown	Japan	🇯🇵	2514	INFOSPHERENTTPCCommunicationsIncJP	false
35.198.197.216	unknown	United States	🇺🇸	15169	GOOGLEUS	false
154.241.231.18	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
102.201.0.33	unknown	unknown	?	36926	CKL1-ASNKE	false
178.114.241.48	unknown	Austria	🇦🇹	8437	UTA-ASAT	false
80.132.249.126	unknown	Germany	🇩🇪	3320	DTAGInternetserviceprovideroperationsDE	false
181.189.142.224	unknown	Guatemala	🇬🇹	23243	COMCELGUATEMALASAGT	false
197.91.89.244	unknown	South Africa	🇿🇦	10474	OPTINETZA	false
156.67.60.64	unknown	Spain	🇪🇸	50129	TVHORADADAES	false
41.210.115.187	unknown	unknown	?	29614	GHANATEL-ASGH	false
197.191.9.241	unknown	Ghana	🇬🇭	37140	zain-asGH	false
41.163.216.196	unknown	South Africa	🇿🇦	36937	Neotel-ASZA	false
197.238.77.132	unknown	unknown	?	37705	TOPNETTN	false
179.93.120.169	unknown	Brazil	🇧🇷	26599	TELEFONICABRASILSABR	false
156.174.55.149	unknown	Egypt	🇪🇬	36992	ETISALAT-MISREG	false
41.169.50.107	unknown	South Africa	🇿🇦	36937	Neotel-ASZA	false
65.12.15.113	unknown	United States	🇺🇸	6389	BELLSOUTH-NET-BLKUS	false
156.144.112.196	unknown	United States	🇺🇸	3743	ARCEL-2US	false
197.81.28.100	unknown	South Africa	🇿🇦	10474	OPTINETZA	false
197.67.168.126	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
96.214.8.56	unknown	United States	🇺🇸	7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
90.27.204.129	unknown	France	🇫🇷	3215	FranceTelecom-OrangeFR	false
197.165.56.23	unknown	Egypt	🇪🇬	24863	LINKdotNET-ASEG	false
156.254.22.239	unknown	Seychelles	🇸🇨	394281	XHOSTSERVERUS	false
41.195.174.174	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
126.14.53.29	unknown	Japan	🇯🇵	17676	GIGAINFRASoftbankBBCorpJP	false
41.138.189.41	unknown	Nigeria	🇳🇬	20598	CYBERSPACE-ASAutonomousSystemnumberforCyberSpaceIL	false
156.31.97.54	unknown	Brunei Darussalam	🇧🇳	34542	SAFRANHE-ASFR	false
197.70.186.123	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
223.33.122.199	unknown	Korea Republic of	🇰🇷	9644	SKTELECOM-NET-ASSKTelecomKR	false
104.88.11.46	unknown	United States	🇺🇸	2914	NTT-COMMUNICATIONS-2914US	false
41.98.223.110	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
44.119.187.72	unknown	United States	🇺🇸	7377	UCSDUS	false
19.166.233.106	unknown	United States	🇺🇸	3	MIT-GATEWAYSUS	false
208.62.239.127	unknown	United States	🇺🇸	6389	BELLSOUTH-NET-BLKUS	false
107.247.243.54	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
41.82.166.190	unknown	Senegal	🇸🇳	8346	SONATEL-ASAutonomousSystemEU	false
75.161.159.225	unknown	United States	🇺🇸	209	CENTURYLINK-US-LEGACY-QWESTUS	false
154.230.147.127	unknown	Uganda	🇺🇬	37075	ZAINUGASUG	false
41.92.95.74	unknown	Morocco	🇲🇦	36925	ASMediMA	false
197.70.138.237	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
41.251.205.235	unknown	Morocco	🇲🇦	36903	MT-MPLSMA	false
41.66.91.111	unknown	South Africa	🇿🇦	22750	BCSNETZA	false
41.219.35.198	unknown	Senegal	🇸🇳	37196	SUDATEL-SENEGALSN	false
163.4.152.107	unknown	United States	🇺🇸	17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
44.199.68.226	unknown	United States	🇺🇸	14618	AMAZON-AESUS	false
144.152.86.32	unknown	United States	🇺🇸	58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
197.250.1.128	unknown	Tanzania United Republic of	🇹🇿	36908	VTL-ASNTZ	false
156.158.248.172	unknown	Tanzania United Republic of	🇹🇿	37133	airtel-tz-asTZ	false
59.172.201.214	unknown	China	🇨🇳	4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
205.241.62.172	unknown	United States	🇺🇸	3364	CSDCO-ASUS	false
197.179.254.35	unknown	Kenya	🇰🇪	33771	SAFARICOM-LIMITEDKE	false
201.21.20.72	unknown	Brazil	🇧🇷	28573	CLAROSABR	false
197.10.137.63	unknown	Tunisia	🇹🇳	5438	ATI-TN	false
58.203.24.157	unknown	China	🇨🇳	4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
41.65.235.145	unknown	Egypt	🇪🇬	36992	ETISALAT-MISREG	false
41.122.213.33	unknown	South Africa	🇿🇦	16637	MTNNS-ASZA	false
115.136.177.106	unknown	Korea Republic of	🇰🇷	17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
156.188.232.23	unknown	Egypt	🇪🇬	36992	ETISALAT-MISREG	false
41.242.158.94	unknown	unknown	?	328594	SUDATCHAD-ASTD	false
201.174.98.231	unknown	Mexico	🇲🇽	32098	TRANSTELCO-INCUS	false
131.97.38.24	unknown	Sweden	🇸🇪	10631	GEORGIA-STATEUS	false
156.155.119.251	unknown	South Africa	🇿🇦	37611	AfrihostZA	false
156.17.39.226	unknown	Poland	🇵🇱	8970	WASKWROCMAN-EDUeducationalpartofWASKnetworkWroclaw	false
176.191.175.199	unknown	France	🇫🇷	5410	BOUYGTEL-ISPFR	false
156.147.203.60	unknown	Korea Republic of	🇰🇷	4668	LGNET-AS-KRLGCNSKR	false
41.85.112.181	unknown	South Africa	🇿🇦	328418	Olena-Trading-ASZA	false
197.89.172.98	unknown	South Africa	🇿🇦	10474	OPTINETZA	false
182.119.170.146	unknown	China	🇨🇳	4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.130.61.222	unknown	Australia	🇦🇺	133612	VODAFONE-AS-APVodafoneAustraliaPtyLtd AU	false
155.194.120.135	unknown	Canada	🇨🇦	8698	NationwideBuildingSocietyGB	false
180.187.203.78	unknown	China	🇨🇳	4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
41.103.227.4	unknown	Algeria	🇩🇿	36947	ALGTEL-ASDZ	false
41.91.11.130	unknown	Egypt	🇪🇬	33771	SAFARICOM-LIMITEDKE	false
126.184.84.191	unknown	Japan	🇯🇵	17676	GIGAINFRASoftbankBBCorp JP	false
41.38.134.238	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
54.103.47.156	unknown	United States	🇺🇸	16509	AMAZON-02US	false
24.246.58.91	unknown	Canada	🇨🇦	5645	TEKSAVVYCA	false
62.71.201.238	unknown	Finland	🇫🇮	1759	TSF-IP-CORETeliaFinlandOyjEU	false
156.99.130.47	unknown	United States	🇺🇸	1998	STATE-OF-MNUS	false
197.169.67.100	unknown	South Africa	🇿🇦	37168	CELL-CZA	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
197.47.156.113	4Vp1NlOQKm	Get hash	malicious	Browse	
5.172.117.173	ot0uxrCL6q	Get hash	malicious	Browse	
98.150.50.118	BunfEuaoK5	Get hash	malicious	Browse	
41.14.214.62	frosty.x86	Get hash	malicious	Browse	

Domains

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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MTNNS-ASZA	x86	Get hash	malicious	Browse	• 197.73.219.98
	FWsCarsq8Q	Get hash	malicious	Browse	• 41.195.174.105
	sora.x86	Get hash	malicious	Browse	• 196.30.233.243
	p6j5MzMpDW	Get hash	malicious	Browse	• 197.76.213.119

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BMP4Nk5TTq	Get hash	malicious	Browse	• 41.195.197.59
	PFD33mzc5l	Get hash	malicious	Browse	• 41.119.144.184
	tqQd9hibj0	Get hash	malicious	Browse	• 41.121.172.228
	x86	Get hash	malicious	Browse	• 197.66.231.49
	arm7	Get hash	malicious	Browse	• 197.73.219.37
	arm	Get hash	malicious	Browse	• 197.66.206.89
	7qvn4qlmi3	Get hash	malicious	Browse	• 197.73.219.217
	JuofJwjQMT	Get hash	malicious	Browse	• 197.65.82.63
	GRPVtMlbK5	Get hash	malicious	Browse	• 197.69.35.19
	arm7	Get hash	malicious	Browse	• 197.73.244.45
	x86	Get hash	malicious	Browse	• 197.71.38.238
	arm	Get hash	malicious	Browse	• 41.127.73.165
	6hIVFnTCbu	Get hash	malicious	Browse	• 197.66.206.88
	arm7.light	Get hash	malicious	Browse	• 41.121.68.114
	pandora.x86	Get hash	malicious	Browse	• 196.30.145.214
	x86.light	Get hash	malicious	Browse	• 41.122.114.224
TE-ASTE-ASEG	x86	Get hash	malicious	Browse	• 41.37.180.48
	FWsCarsq8Q	Get hash	malicious	Browse	• 197.44.77.115
	UVcZqHn4.exe	Get hash	malicious	Browse	• 156.207.27.79
	8d4VwKgV.exe	Get hash	malicious	Browse	• 156.207.27.79
	p6j5MzMpDW	Get hash	malicious	Browse	• 197.55.82.102
	BMP4Nk5TTq	Get hash	malicious	Browse	• 41.40.226.122
	B6WwgS8sUq	Get hash	malicious	Browse	• 197.45.249.129
	PFD33mzc5l	Get hash	malicious	Browse	• 41.237.139.123
	tqQd9hibj0	Get hash	malicious	Browse	• 197.55.181.84
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 156.207.31.10
	buiodawbdawbuiopdw.arm7	Get hash	malicious	Browse	• 197.49.247.241
	DHLx36.apk	Get hash	malicious	Browse	• 41.41.255.235
	x86	Get hash	malicious	Browse	• 197.47.0.177
	arm7	Get hash	malicious	Browse	• 41.239.14.35
	arm	Get hash	malicious	Browse	• 197.44.29.239
	7qvn4qlmi3	Get hash	malicious	Browse	• 41.44.132.72
	JuofJwjQMT	Get hash	malicious	Browse	• 156.223.144.240
	GRPVtMlbK5	Get hash	malicious	Browse	• 197.53.120.110
	arm7	Get hash	malicious	Browse	• 156.199.251.158
	x86	Get hash	malicious	Browse	• 197.40.144.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8662467bc96db2d387755570446a7946	mirai.arm	Get hash	malicious	Browse	• 162.213.33.108
	2j7dEG022b	Get hash	malicious	Browse	• 162.213.33.108
	sora.arm7	Get hash	malicious	Browse	• 162.213.33.108
	sora.x86	Get hash	malicious	Browse	• 162.213.33.108
	sora.arm	Get hash	malicious	Browse	• 162.213.33.108
	EHqBakwhNU	Get hash	malicious	Browse	• 162.213.33.108
	vq0sPlNJDK	Get hash	malicious	Browse	• 162.213.33.108
	w07UCYGzBe	Get hash	malicious	Browse	• 162.213.33.108
	Rry5mHEWuH	Get hash	malicious	Browse	• 162.213.33.108
	ofgE8wetW4	Get hash	malicious	Browse	• 162.213.33.108
	0bqzNIp9PV	Get hash	malicious	Browse	• 162.213.33.108
	yjJXz4a3u6	Get hash	malicious	Browse	• 162.213.33.108
	g3wyMOTecE	Get hash	malicious	Browse	• 162.213.33.108
	7k6FKvDl0x	Get hash	malicious	Browse	• 162.213.33.108
	KSzA1ujvlV	Get hash	malicious	Browse	• 162.213.33.108
	y66dLhUn0G	Get hash	malicious	Browse	• 162.213.33.108
	5j9ZIHs8fD	Get hash	malicious	Browse	• 162.213.33.108
	1isequal9.arm7	Get hash	malicious	Browse	• 162.213.33.108
	1isequal9.x86	Get hash	malicious	Browse	• 162.213.33.108
	1isequal9.arm7	Get hash	malicious	Browse	• 162.213.33.108

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/5426/oom_score_adj

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

/proc/5472/oom_score_adj

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

/proc/5472/oom_score_adj

SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0

/proc/5475/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0

/proc/5477/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB 99
Malicious:	false
Preview:	0

/proc/5479/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB 99
Malicious:	false
Preview:	0

/proc/5481/oom_score_adj

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

/proc/5481/oom_score_adj

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

/proc/5483/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/5486/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/5632/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/5662/oom_score_adj

Process:	/usr/bin/dbus-daemon

/proc/5662/oom_score_adj

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

/proc/5665/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/5667/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/5669/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/5671/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/5673/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/5676/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/5980/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/5995/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/6208/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/6277/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	0

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:EDvn:EDv
MD5:	C6F297DD663BE725ECA19F84A45F3BF0
SHA1:	D4DA042A0AD6A9ED9EF685474E2C1B322EE66C30
SHA-256:	EA8F28B79F65E166127727E46C60FD8E6F8AB5470AB2C64E5DEC9D8F3BAC0D93
SHA-512:	FFE1409CED3FC6D6176D48832E0C281C37177D7B322B47AC533AF3BC26E8ED5B3C7E9455588AB5A26DBE6C1EE434AFC1303A3318838622B125751C8A6398092
Malicious:	false
Preview:	5426.

/run/user/1000/pulse/pid

Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:FWo:f
MD5:	8AC6ADC9BBBE1BB00BFB1EF091043C7B
SHA1:	1728E9871F04C6B62E422EF1FFAA69967CA9270C
SHA-256:	2D9446EBF2F0AD5AC322B4457D1E06F5DE558615F00CEE93702DA3AA28DD1B0A
SHA-512:	42FDF92389708C783110C86794F6AABF061AFFFDE388AB4D6ADB32387D0008FCE9040F702DEDAD3348B38CFEC2E383CD80C4F04B2225F7491B17CC510AD914 D
Malicious:	false
Preview:	5533.

/run/user/127/ICEauthority

Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	6.035077250418384
Encrypted:	false
SSDEEP:	12:OxPv92veY+v5xP3PQlveY+3v0dokxP5mhijveY+5tWmxPwWoveY+wcZVveY+wYvr:wk/wqrjxz
MD5:	4831A5B3B5525E7DE15392889E615469
SHA1:	FB49C64DB20B05C8431E30C8A288BFB1B44D3305
SHA-256:	CA250CDBF471B5DBEF131C9BD0C0B6AE82FE87681F6BEA1EBC538DEF5C11727F
SHA-512:	95B04086A8DA5E30B3CF73449325A4640A41B9FFD9E59E84A1D65AE1158810B8483A3F32C4AB9BCD217D7B5AF73402EB87F0564740435F38E8609B3525F43F8F
Malicious:	false
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5570..MIT-MAGIC-COOKIE-1..a6Q........./...XSMP...#local/galassia:@/tmp/.ICE-unix/5570..MIT-MAGIC-COOKIE-1...Dr.O.y...... ...ICE...!unix/galassia:/tmp/.ICE-unix/5466..MIT-MAGIC-COOKIE-1..v.]..c.E.9$9;..j..ICE...#local/galassia:@/tmp/.ICE-unix/5466..MIT-MAGIC-COOKIE-1..d........... '..XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.......A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....o.(R...}.9. ..ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f........E..c ..XSMP...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... ......Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,.:B.o. .....ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN.....N +..$..XSMP...#local/galass

/run/user/127/dconf/user

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

/run/user/127/gdm/Xauthority

Process:	/usr/lib/gdm3/gdm-x-session
File Type:	X11 Xauthority data
Category:	dropped
Size (bytes):	104
Entropy (8bit):	5.0217563256604105
Encrypted:	false
SSDEEP:	3:rg/WFllasO93QmEoTBJEENWFllasO93QmEoTBJn:rg/WFl2pE6LNWFl2pE6J
MD5:	BFB4846D0842BAA24217EE518170ECDE
SHA1:	03DB41C6763ED2D6D4D9C18B6147EF07CE63E613
SHA-256:	FE1CA8E9FE01D6298E69B6673EFF8650E391CB12ECBFE5B4E6F71A79D60F7814
SHA-512:	FFA7DE3CD1E0AE9E21174AF1995530BFB0CE0B626D0907027DB02D31664BFE21B193F866BA8EB8B49FDB08EB3EE237E755142EE34B4E8EC8A744DC23CCE49 BC

/run/user/127/gdm/Xauthority

Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1...u...}..6.....xn....galassia....MIT-MAGIC-COOKIE-1...u...}..6.....xn

/run/user/127/pulse/pid

Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:Jc2n:v
MD5:	59EE1008643E6413FD61777E724AE4E5
SHA1:	D3CBA3FB10ABF6337FC36122A501A9A20C4B8C5F
SHA-256:	2BFA1F32A46C3B38A3815631C5F03562A425C0179F1B9C3E0AB2374BDD408953
SHA-512:	6BFB2601A8F308DD276CCED55D8A8F1B334A95AE3CC7D5342B1CAF82A16E1CC31F61427EE25F3FAA5C454C1AC65CD7B4A306AAD6550B5D3C8BFD9B8DAD2302A
Malicious:	false
Preview:	5991.

/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/man/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	4.657516417799966
Encrypted:	false
SSDEEP:	6144:rb7cWWov4H5N80nuDSyvxYCWZ0/VmpRELAR/QuU/MzUCl1NZ:H4WWoGgvSiOp2kl
MD5:	0C99179B6C5CFE82203424AD7DAD0D8F
SHA1:	CAC50B64B1352723FF8F58BB1B103B93C396539B
SHA-256:	CEC6859D12C6A981ACA4D7C88F6E62E9616FB4D765C4A52147A7DA7BAD4F2420
SHA-512:	4226FDE9F558FFEF2107C330DB942E7E665C51C520A840221541AD255D0995AF64101C69D42C4BD43037364CC4D152851625A53DC56CC188DC28A3DC8C5602F
Malicious:	false
Preview:	.W.. ....

/var/cache/man/cs/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384

/var/cache/man/cs/5316

Entropy (8bit):	1.6070136442091312
Encrypted:	false
SSDEEP:	48:bhVGQeUzGLIsWUMZJ5CggJHtheYdiKNHTlJ8NK:bhVGaGLIWMZXZgxeYtzll
MD5:	D0CA2EBA9E7A17D4680AA9DDC5F88946
SHA1:	270F443EFF85209052AE8FFA86660AFB0FAAD39B
SHA-256:	9504DC65F8B4E057D0939FA3B2C640FC703D0290EE19381836BAA5EB3EFBADBD
SHA-512:	9F999B0467E396E78A91F0BFE56E191DB9D9AFA6DC47858F3427CB44A39D5A13A206542A471CE15C8851674A234B9A7A49AAB7E6D5AF8D080BBC99C2BA3C56D 8
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/cs/index.db.S87xfb

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/da/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.24195239843379
Encrypted:	false
SSDEEP:	96:bhHY2DzMnpU0QMiloesQdUTn3WVE0UnknJfsWdv0SBpEVvsb6eZeGfRL+:dYKM+oagn3WW5nkniWdv0SAVE6eZee6
MD5:	4DF08004EE4C5384C02376841F2B50BC
SHA1:	C02E58212CA012913390B4C1CCD64DD3353009EE
SHA-256:	F4D6A62A734E2844B99F3AD0EB480373AFBE56B29C0CFC9C70D9DFDF19D95C02
SHA-512:	6146001CA7028F58595235F244AE8FC4ECAEA3E95C83276514FC704E91B7596678E74CDE9963D680F2493F9C04AFDEBC4DB5094E2AB7C1A949E9378307AE0116
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/da/index.db.8cAzyb

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false

/var/cache/man/da/index.db.8cAzyb	
Preview:	.W..............................@.. ....

/var/cache/man/de/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	4.163065551949528
Encrypted:	false
SSDEEP:	768:gMGrknsA3KVtOOcmGMrTJDEEf5R6OHiiVDdtq5:/GrkncXD+qxHiGLq
MD5:	2D1A45A997D2119DE40DA0612C4B3633
SHA1:	3E01DFF504BF63C935D84D153446C8C7BA979A77
SHA-256:	E8575B7F765D500DCFE41379EBAEC61DF21025E47D6B6DFC63350190EAF0C7DE
SHA-512:	CB6FB238C0D9808DB7BC95FD8B832489932EFEBFABE6A6195054B176B2C7177353BA394157A27E0EC50AFB773FB3711E34243A4C9F80ACFE056C495A93BEE4A 2
Malicious:	false
Preview:	.W.. ....

/var/cache/man/de/index.db.dqh7ma	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.20558603354177746
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	55880A8B73FD160B73198E09A21C83DB
SHA1:	5EB780702D2501747AF46F7525EF5C635EC5E64C
SHA-256:	66BD4C98AF40E2E208AC102ACD0F555A6C118E7258D91B833BE1D53EBFFB7BBB
SHA-512:	388924B8CAE80CCA6CA8E5109D0239A963A66CC0454450223EC7FB2A188F6F05E49632E535DC06E49DF6D007B221AA6B3D5F23C80203BCC861FF95EFA10AC1F
Malicious:	false
Preview:	.W..............................@.. ....

/var/cache/man/es/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.469907427008948
Encrypted:	false
SSDEEP:	96:bhj9SeW/8iDdO/tktuGWTaZxzn3zbHGc2WjAXGBCgfd6Dgzs30z8ztvpWF4DXst:99PGo9Tmn3zbNBSw/fd6Oz8ztQSDXo
MD5:	3DBF4FF017D406F407BFBC2011BCAE9E
SHA1:	FF64864ACA18DFA7869715CE8AA5ECC3DABA54B6
SHA-256:	640C040F364061A5825E913682798C9BC8E1081088894D3FEB2C3EC39D02A379
SHA-512:	3DCC8F432487C532A1F69D321EB57EFE5CFE65AA3C99B81EA1A56613F8F460EA9ED7D2031615F2E60A3F2EE279D411848E5387CC8B8D5F28D8F8D0055D72489
Malicious:	false
Preview:	.W..............................P... ....

/var/cache/man/es/index.db.rN2ivc	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480

/var/cache/man/es/index.db.rN2ivc

Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.............................@.. ....

/var/cache/man/fi/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.5882948808594274
Encrypted:	false
SSDEEP:	12:Ey20yaajjjjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjjjjjjjp:bhjz+9Ab
MD5:	09F6ED1A60B8A4203EA97CF5926C6AFF
SHA1:	C28F4E393D55AD057E3C7608741904B796F67076
SHA-256:	56664D61D0BB8BF34CCA28C73CB314CB73EA1C4FAC64D2208B43F63C009FC855
SHA-512:	476EAE37D827C8BB322213799AB52DBE8FA43274DB3447BC5FEDFED64ECCEAF2C11DA375FDA09B37977D03CA1910E22443B22A3EEA875CE6F3BC698F8ADC 0E2
Malicious:	false
Preview:	.W.............................@.. ....

/var/cache/man/fi/index.db.a9Cx89

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.............................@.. ....

/var/cache/man/fr.ISO8859-1/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20yIpyjjjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003 B03
Malicious:	false

/var/cache/man/fr.ISO8859-1/5316	
Preview:	.W..............................@... ....

/var/cache/man/fr.ISO8859-1/index.db.847Wfb	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/fr.UTF-8/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20yIpyjjjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003 B03
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/fr.UTF-8/index.db.4XiuZc	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/fr/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960

/var/cache/man/fr/5316

Entropy (8bit):	3.830233312985169
Encrypted:	false
SSDEEP:	768:A4VX6Bd+dla5HmdT8qHl87BaIPay4uz8HksGHnwNO:A4ROd+dStM83PavGHC
MD5:	A6054B911543D2220BFADF8041BF7DF0
SHA1:	A513A0827A32E39CE67BDEF86FB01A1D54C040AF
SHA-256:	3F78DFE837F755D1B4830CB9E7B119E88B0987DAEC1965BA488B9C53D6B4D1A2
SHA-512:	0F6604BD010506711936B3526CF3816419296A284814C2776033E3F8F069DE7AA80D3BB04D45E2EF58E8E9D39FDDCEADDF6B94707078E7A2FCFD685A88D5EF4
Malicious:	false
Preview:	.W.. ....

/var/cache/man/fr/index.db.FOdfUc

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.22208993462959856
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	425CB57CD9B42556C8089FE7A7A3E495
SHA1:	4F33F9A9897218FDED958FD8F8D7AF7CD8BC48F3
SHA-256:	85E01EFF2AC0C83C827E118D5CE2CD1E1A19E059688B6E0D09CB3CC131F065D3
SHA-512:	8C7D4DACF5C5C5C4B78775048427AF99ED8057590AA3A69FD5B3F875B6DDD249A6DB0AF3A51BB96A7F629D1017B272317583A8DFF89FB3968FFE2F246F040F3
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/hu/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9419610786280751
Encrypted:	false
SSDEEP:	24:bh04IR9rYz9kvNQFl46MdnqfPE9eTuF0Ce:bhXIHakVQmnqXqeT/Ce
MD5:	18F02B57872A97DE1E82FF5348A5AF1B
SHA1:	52F332343B120B1C950AC02B3C923556C70DC62A
SHA-256:	5C605DE68B3E05754698485F73413F4052AEA8C3AAE6012AC6416B3B6B056DF7
SHA-512:	E33A8412F52D26BDE55E4D72E0D9D09EB777F4B882F5BB1C4625AB392EE321D6ACD8795001BF50CCDACFAC131A1263B1398F208799F753554C43349136EB8BE C
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/hu/index.db.0pz938

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false

/var/cache/man/hu/index.db.0pz938

Preview:	.W.............................@... ....

/var/cache/man/id/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.309811236154278
Encrypted:	false
SSDEEP:	48:bhESUeDVrWTVd5ekRv/KSmGWqR0VouC4btU8IzTC74ExJKGtII:bhEVeBqTVdAcn3Iowl4UBtx
MD5:	3AFDA1B0F729816929FF7A6628D776D5
SHA1:	5982940A5782F11AEB5BF859C055DE3FEFBDF5DB
SHA-256:	77809D5F38F6D96A2E8BA9BE0DFBB16C10B6B1FF7D2BA1DD5FB9437F73C47E7F
SHA-512:	6D4CE03475C68EDC0AE928E7F65BB8C06198721146A1266F55455AF3D5E24F44A569E007C0DC44BC7745C1573DBC7F02B8C4094F9BD97FAF6A0B5894BE0E07E
Malicious:	false
Preview:	.W.............................@... ....

/var/cache/man/id/index.db.n5U5qc

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.............................@... ....

/var/cache/man/index.db.1rTuKc

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	0.022159377425242585
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	2E442DBA85DEDFDCB07090FDF9DE90D0
SHA1:	02658086E93854D13D82B1F0D80F4B78D26DCA51
SHA-256:	62406BFE7657964E490DE65A0007F7C1D59B62B2B9AD35BA55BA219673378848
SHA-512:	FDBBA0DEF310CF7DBF448CFB6E5C9CDCEFBF6A0CAEB26CA3AFA91A388FBA10A9E77BCC27CA9B0AEA2A7B67F964849E147FB44862C7394C2C7CDCB572C06 FCB05
Malicious:	false
Preview:	.W.............................@... ....

/var/cache/man/it/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480

/var/cache/man/it/5316	
Entropy (8bit):	3.3621193886235408
Encrypted:	false
SSDEEP:	384:Jtp0q5d98n3SaMfhtxfmbMy+HseeNwoMbHf:JDd9QSBf
MD5:	B228DE097081AF360D337CF8C8FF2C6F
SHA1:	7DD2C4640925B225F98014566F73C35F4E960940
SHA-256:	1056CECADA78542B173EE469C9BEAF61F81298EBBD21B54EA6EE449028E18B3F
SHA-512:	F61D7F9040E452C4B1B77F3657BE4252475C3BF23D78EED903A5E55FA97BA0571BA3AD90DBA7F77C334DF5B721F909B12720515034421A4AAB0450D1D43B32E4
Malicious:	false
Preview:	.W.............................P.. ....

/var/cache/man/it/index.db.E7jVrc	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.............................@.. ....

/var/cache/man/ja/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.667488020062395
Encrypted:	false
SSDEEP:	192:CF4pPRfAgFn35FF1veUMjGiEGBuPhiB0PUKwA+U:5PRfAgFn35MSeAPUjN
MD5:	D3CD7D67F8155491493BB7235FB9AA57
SHA1:	5A7AE62A7AFE50EFCCED06CBD56AE2A0A284EFF3
SHA-256:	6958349ECA637F99AABC419B5E402CFB50BC5B8867F31BCB67F064F47A209929
SHA-512:	1168BF697CDE563F7D82A71EAE1CD496EA81D178B26F87EAAF2EDEED13274B1E3500CE1C981647717598495EBE1FF8F8AC54AD33547506E566C925D7002F5CF F
Malicious:	false
Preview:	.W.............................P.. ....

/var/cache/man/ja/index.db.avEphc	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false

/var/cache/man/ja/index.db.avEphc	
Preview:	.W............................@.. ....

/var/cache/man/ko/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.7847786157292606
Encrypted:	false
SSDEEP:	12:Ey20yYn0jjjjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjjjjmjj7:bhXYznMk31RFe6f
MD5:	FBA25855E1C99D8F87E8AC13E2E2ECB1
SHA1:	D99351AC40D6CC4C9BE54E0E018C44A9A88983D7
SHA-256:	C0E18ED1CEFF427FD4D57D1B79CE1AF7320AC8453BAF8A0349C08267464C4D71
SHA-512:	0969DF6506E083A4995A18518BC3C4472157E7790EEC26C08221B0FC6DE9C7DA0ADB11CF92C56BC35B89BC60447F3D991F935E352552B58FB9BD1D4B2579FBE
Malicious:	false
Preview:	.W............................@.. ....

/var/cache/man/ko/index.db.yjzkp9	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A24930809
Malicious:	false
Preview:	.W............................@.. ....

/var/cache/man/nl/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.554204221242331
Encrypted:	false
SSDEEP:	192:H8Y5a2oquB2aCYn3lvu3whjXVobdbs7dq1KJGbtf0Hoa:hoquYaCYn3Q8jXqbdbs7dGbKHoa
MD5:	27FED1CA8EB0101C459D9A617C833293
SHA1:	503B2A3E33FE79FF2CD58F831ED33DB358849BEA
SHA-256:	C3033C4F7CF0D6108611EF5A62CA893F98EE6463DDCFF7100D3BAFDEB0036D9E
SHA-512:	7BD630F5E0C5A91C34D2E48D0053923C9F2F5BAA07D21FDA79E60F3AFDF759E594E6639562C1F3EE68DD080D417009DC3AFB7DA534E3B8C29FF7B10438C3FD E
Malicious:	false
Preview:	.W............................@.. ....

/var/cache/man/nl/index.db.1IS3J8	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384

/var/cache/man/nl/index.db.1IS3J8

Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/pl/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.880948418505059
Encrypted:	false
SSDEEP:	192:7Sf8026LXqn3ZTV6pXAmA44BRqvc3X3GVAjvAk/AvdWjWftxA:E802uXqn3/6pxARqr8kdWjW1
MD5:	37CEBCD3F5BF6322785FFF568EE33131
SHA1:	201298C827C77C60CD314BF721DC4C27EF95BD64
SHA-256:	012C5597C5DD8654EB14432AFCEFD9B131F2CE75AD21488991A5A688929AAEA6
SHA-512:	CCC8A8CCF4ACA332CAF610155DE9E7C4A12D1C45C98D20766B86098A3D2EF332189F159E3956944CD302DF652FE7A6F0D07CA39CBE7DF4A655D32114524875
Malicious:	false
Preview:	.W..............................P.. ....

/var/cache/man/pl/index.db.ebxeRa

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/pt/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.4110695640960995
Encrypted:	false
SSDEEP:	192:mva8yGn35+0+eo8TAnBW4VppKP8qtRJI:Sa8Rn35+peo8T8V/fqlI
MD5:	782FF89B6FA5932F7019AF9CF3F82E43
SHA1:	2ECE8DC134E3A292E2545AA2DCD24114A5FC5749
SHA-256:	01E77D9235C524F2A61EA03953607C13831C391A5B9AB0D9094F9C38F0EEB02E
SHA-512:	2305BEC024CA5D8B43267F5487B02081A0A746B73608E11217D19C91AD857B6A5D8E935194AC4228DA3A5383086E60D593095309E64BAF38841A6E32D7EA7805
Malicious:	false

/var/cache/man/pt/5316

Preview:	.W..............................P... ....

/var/cache/man/pt/index.db.PniTJ8

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/pt_BR/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.7510008687365202
Encrypted:	false
SSDEEP:	48:bhX6G+IwvnUZe4Gv/KSmGROqAQAuSe0dDOfInYbmucrm3QEAvJBFIz:bhq5bnUY4Gn3P+/Z1tvJDQ
MD5:	A11F5E85A2A07AF84255570AE29318FB
SHA1:	D06BF25E5FD4A17BCF7C5BD77ACD747F0FE181E8
SHA-256:	8FFA8BC408B254217275A622D054853CB72B08409A11AA49C4C664C0DABFB62F
SHA-512:	059F3CBC93750B68942D88EDD4AD2531B2291CEC421EB903280B9105010D1C8AD70F9F3CFA1B1A50D5110DCBFDB807A6E7A3F9EBC9A48AC8C3A49DEC4B6B3 99
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/pt_BR/index.db.JS3Ci9

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A249308
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/ru/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	24576

/var/cache/man/ru/5316

Entropy (8bit):	3.440634655325007
Encrypted:	false
SSDEEP:	384:SpjHrhEon3PRekEF3PS6y13Vi6w5TlmmcOB:Q3hNEk23MuxrB
MD5:	DF5C1114538C5D8EA1EE929FFAC24E3C
SHA1:	B6331AF77566B63EA8204BE85F5DC99FAF51479E
SHA-256:	F238C75DAD82E10AB011A9BF79775B2A5F5889644A5A06835933340845A08555
SHA-512:	9514A424CC2A9290F749F527F515B35E45C6A829CB3930DBFB39DC9D70A684640A31686EC77258FF285FE89B6DD44BB01A478848FF9B3EBD764741A6F7856704
Malicious:	false
Preview:	.W............................`... ....

/var/cache/man/ru/index.db.ryY3Ia

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	0.3337394253577246
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	5B66CE03BFE548DEE335E0518E4E0554
SHA1:	65397845DC679AA972454B0FF237A513C0F490CB
SHA-256:	C38BB21B1D92166794DC09807C9A55B67B0A760C684FEEDD0C931F8415DD6D29
SHA-512:	A31C3D23F25607333250443490F0EE295BB702B46A636905FD413E8AEAA8ED23AAB42106868D2938718555C9DEEFB69FB416CAF5228A422F64D6CA8DB438FEE8
Malicious:	false
Preview:	.W............................@.. ....

/var/cache/man/sl/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.8558400366712392
Encrypted:	false
SSDEEP:	12:Ey20y8jjjjjjjjjjjjjjjjjjjjjjGjjjKuV0jjjjjjjjjjjjjjjjjjjje:bhaVZjx6ot7m13SmZQs
MD5:	67697BEA7C23E4805A82FE9755BB3CAE
SHA1:	14ACAFF0BECBDB116E4C0BC329E59DEF68CF46D1
SHA-256:	553DA7FF76999B7CCC4450498B11E6BD98B3B1E5FF81D82A53568F84B0D270D5
SHA-512:	D966DD6430003E708C6EE10764DC072A1ED0A252E6E1C822CBD28271A2EDD4B1F61C7F9AA7D1D442D6175791A104A365DE25B9C2598500AE705C9250C8BA46A 1
Malicious:	false
Preview:	.W............................@.. ....

/var/cache/man/sl/index.db.UHwNP8

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A24930809
Malicious:	false

/var/cache/man/sl/index.db.UHwNP8

Preview:	.W.....................................@... ....

/var/cache/man/sr/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.3868484511023333
Encrypted:	false
SSDEEP:	48:bhLSUCt/WFekRv/KSmGWqApnEVyfNsu+tBNGg2PgULLE2vRy2QwfoQEDiR2e3iRj:bhLVC48cn3Vu2FtBv7AtboQIqb3qwK
MD5:	0DD75ECC81E4E564EA56A57FF32A24D3
SHA1:	859C0FE5F86A2C5A32BAD7920787BE845F34C4FB
SHA-256:	DB778B175D19DEFA4180D0B12D675AD0B8B22CC4BB77702D9EC8510F894EB3B1
SHA-512:	7B0C56A76797383527509F8036EB4911F8925E7ACC005CDC3269F0A43231479E3A0A9887BF4D2979F05CBFE18324997DEF715FDA6921EEF827B385C9D902C708
Malicious:	false
Preview:	.W.....................................@... ....

/var/cache/man/sr/index.db.MzE41c

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....................................@... ....

/var/cache/man/sv/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.5432558448090097
Encrypted:	false
SSDEEP:	96:bhk/+fz7b9ldxbe2Vn3iwkVJIB0D6c6aZ4+1Wrzbxpl4/tMe1:imrn9lHbe2Vn3iwKhD6cvTAbl4/tMe
MD5:	D97454D6B1F39F39966A809BCA3D9647
SHA1:	276931CED8F34B7651C1BDFC8522FF0560E2C377
SHA-256:	DCB8CE7F4F21595D851100F315C56B717541DB898AEB9ED9C0CCC9FF217A5801
SHA-512:	3E014F3EA8EEE79B87726EDA6291AC2D0BD9B22803EE848F61CA2AAD39D5FB87704410C57C648EE4AF8A1B78EFB0D766524F6DB750208C9BAC346079FD8EE6 9E
Malicious:	false
Preview:	.W.....................................@... ....

/var/cache/man/sv/index.db.ECnlfa

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384

/var/cache/man/sv/index.db.ECnlfa

Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A24930809
Malicious:	false
Preview:	.W..............................@.. ....

/var/cache/man/tr/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.7558188637474321
Encrypted:	false
SSDEEP:	96:bhWV1OIM7cn3UZiPU1wywyoEpJmz6W2Mzgg:YDOL4n3fPvywrzgMU
MD5:	5F905B930E7310E72BC3DF5C50F8E579
SHA1:	50B1AD3115F095C743CB26F87ECCE406FAC3523B
SHA-256:	1DB72BA77CA01F25CA9768999825D8F97F5ED4D00E17C9130D6F7CDE34130270
SHA-512:	A6066F4DF4097DB93673CD156BBE5F910C3F64D01E1671E481BC9FBDD720DBD6F8CEF337E20404F7C6AE97B2FA1F5E67088041ACBB6EA85D6758924D5740D0 C
Malicious:	false
Preview:	.W..............................@.. ....

/var/cache/man/tr/index.db.0I7tJb

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A24930809
Malicious:	false
Preview:	.W..............................@.. ....

/var/cache/man/zh_CN/5316

Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.6210042560348144
Encrypted:	false
SSDEEP:	48:bh5roGafX8XKu5YIoBHtF2YekDsv/KSmGWNmA/y0uJNI/oyjaOUUfEHKn9nnjoEJ:bhdoLfX8N9oBNF2XFn3UD/9FZiy0aoN
MD5:	39398A15564A55EB7BFE895D7668A5A3
SHA1:	28DA677435B87176E08AFABBF8B51F7B93E22948
SHA-256:	A4C0216476E357ED3A23E71333DBE7DE91E04370EF049032EE8E47BB1EDBD83B
SHA-512:	B4E69212338C742F8C83194552078A86E4BED59375D82563C0B4059B7E0D6A58D6317151AB1F2A6FB20D2FF6DB7C550DF6A6984B2BB873A111D58AF9AEB7D95E
Malicious:	false

/var/cache/man/zh_CN/5316	
Preview:	.W...............................@... ....

/var/cache/man/zh_CN/index.db.k4cNDa	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W...............................@... ....

/var/cache/man/zh_TW/5316	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.0170167917961734
Encrypted:	false
SSDEEP:	24:bhAvIZuF4ptmpzf50dhOv8WvxjMMhFmMKxevOfOots+:bhDi4p+ahOhFFKxewj
MD5:	1FC5F2B98E5BC25B10373353D91B86B1
SHA1:	D848DA35B0731328195D59C1E996B95C4952F1F9
SHA-256:	509FAD18B4454CD70D974755F6156D4A5FA9B960AB9FF468D1FC350F0B64F379
SHA-512:	95BC2E289EDE5D9A3F56C9D8AE9DD13D9379BE2ABF8927CDABBE92B9F57A8EB667E9C08E4DFD82BF9F1F57118CE6E495722ADA2668AFF4FA0540F46C0A6D5 138
Malicious:	false
Preview:	.W...............................@... ....

/var/cache/man/zh_TW/index.db.ygJgQ8	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W...............................@... ....

/var/lib/AccountsService/users/gdm.318TB1	
Process:	/usr/lib/accountsservice/accounts-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	61

/var/lib/AccountsService/users/gdm.318TB1

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.O80OB1

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):	5.155900209820849
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWW1HUqM+GqSe:q5sU3LWfLUDmQymqSFbfomSP0qM+rhfD
MD5:	94C2971C8E24A49FEA121CB493B73290
SHA1:	E0BFCEE9DD79CA68CBF98019C4E37432EBFDE414
SHA-256:	F856401D807D393AF8DAAB1474C2479ADE3C2C845239F301706C1BAC9B78FD39
SHA-512:	2854F04F55509AA9435F668E51A73431D7953F75DC024BC692472E0C6D004D2E6571E761E9C6AE3AAD5B93DD18D2BE9607B663F507B5054CB611BDD3C1058148
Malicious:	false

Preview:	# This file is created by ibus-daemon, please do not modify it..# This file allows processes on the machine to find the.# ibus session bus with the below address..# If the IBUS_ADDRESS environment variable is set, it will.# be used rather than this file..IBUS_ADDRESS=unix:abstract=/var/lib/gdm3/.cache/ibus/dbus-JdCaKVCj,guid=1d3
	2e5b4cd056a0eb7fb00f66170c9ab.IBUS_DAEMON_PID=5784.

/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)

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

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/logrotate/status.tmp

Process:	/usr/sbin/logrotate
File Type:	ASCII text
Category:	dropped
Size (bytes):	1623
Entropy (8bit):	4.775202447060433
Encrypted:	false
SSDEEP:	48:UTREqJFNIEr0kEtEK5Npq4pN7EJNcsXNU3N6NA5YE5xTtNq4wNZNDNU1LN3o9Nc8:+Nrafkotm4pxAxe3MmYqA4wTteJYmNnC
MD5:	D693C9CF5240072B571B46379A07D610
SHA1:	8C5CC0380EAAFE50E5DDDD1B86F05530BF138F24
SHA-256:	98311241C5A43AFE7C1F05EB4DFB20921F4F51C95330EC4945461F1E7CEB28AD
SHA-512:	BB91E75082EC4C253EC0593514B12CDA167E76C18A1E0BB355A002A244C8C124E3FD686E4E738C9B05CD2CD5E825F83CD127CA36F01F26E3540D3CB782AF18 6
Malicious:	false
Preview:	logrotate state -- version 2."/var/log/syslog" 2021-10-21-1:57:55."/var/log/dpkg.log" 2021-10-20-23:57:29."/var/log/speech-dispatcher/debug-flite" 2021-8-20-13:0:0."/var/log/unattended-upgrades/unattended-upgrades.log" 2021-10-20-23:57:29."/var/log/unattended-upgrades/unattended-upgrades-shutdown.log" 2021-9-17-9:23:29."/var/log/auth.log" 2021-10-20-23:57:29."/var/log/apt/term.log" 2021-10-20-23:57:29."/var/log/ppp-connect-errors" 2021-8-20-13:0:0."/var/log/apport.log" 2021-9-17-9:23:29."/var/log/speech-dispatcher/speech-dispatcher-protocol.log" 2021-8-20-13:0:0."/var/log/apt/history.log" 2021-10-20-23:57:29."/var/log/boot.log" 2021-8-20-13:0:0."/var/log/alternatives.log" 2021-9-17-9:23:29."/var/log/lightdm/*.log" 2021-8-20-13:0:0."/var/log/mail.log" 2021-8-20-13:0:0."/var/log/debug" 2021-8-20-13:0:0."/var/log/kern.log" 2021-10-20-23:57:29."/var/log/cups/access_log" 2021-10-21-1:57:55."/var/log/ufw.log" 2021-8-20-13:0:0."/var/log/speech-dispatcher/speech-dispatcher.log" 2021-8-20-13:0:

/var/lib/whoopsie/whoopsie-id.Q53WB1

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):	5.292553560413861
Encrypted:	false
SSDEEP:	384:/VmLyA2nHrMfd3dBd1dJdgdEdhdYdsdmdvdGdEdWdQd/dmdSdEdtdCwdQ9dL1d1G:dmL12Q1z/hbtRIQ6xUoRQoz9UB
MD5:	999F5FA0C803486F8C3C3A811450EE3E
SHA1:	66D150EB379FF2BE0171494DECD426AFE776E99C
SHA-256:	9EF5CF1C245B29800BE5D4FAE5D1891EC9609BB6CB2121C3977C467C922898D6
SHA-512:	8D949AB5883224373AE217B6E99E525847444B952BEAB6D5380496230F2035C1A57E994EC061EDAFD7962612E388E15D16114258B973C77A07BA6A19BC4BE64F
Malicious:	false

/var/log/Xorg.0.log

Preview:	[489.487] (--) Log file renamed from "/var/log/Xorg.pid-5525.log" to "/var/log/Xorg.0.log".[489.504] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[489.513] Build Operating System: linux Ubuntu.[489.519] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[489.527] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[489.541] Build Date: 06 July 2021 10:17:51AM.[489.547] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[489.552] Current version of pixman: 0.38.4.[489.558] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[489.562] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??)

/var/log/cups/access_log.1.gz

Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Wed Oct 20 23:57:29 2021, from Unix
Category:	dropped
Size (bytes):	193
Entropy (8bit):	6.881791153868733
Encrypted:	false
SSDEEP:	3:FtvlfrERm/n+UlBKBUEaB5Jl/DzKY/OEIEPXw3wy5ePPVymeRfafyG3:X9X+UfTlDDzKYGEpPzye3chA3
MD5:	CE81415B794691356A0651FEC147B26D
SHA1:	4EEFFC5A0F4CEF663B1F01659D4BC055393B7084
SHA-256:	8D82E19B086E33F9459F24C32D8CF1C309344F5CE228165F211A012C14211D50
SHA-512:	BABA6FA5794AAB0B57A36E64B78093181491744C07875963188716082F49BC26998B7992ED5BCDCFDDBB215413104170CF15800A73499CDE02A032679C82326C
Malicious:	false
Preview:	.....pa......0.....a5...$...A..q.Zbc.K......$1..._~Kj.O....,x.'..e%....K8.e7H....[.O2.......!j.z.....Ay3EC.@...!..e.:..,.;<..Q..-X^lz.. 1.zpJ./g..D._i-.!)k..L{O.9.l..=...^..xo;...*...

/var/log/syslog.1.gz

<table>
<tr><td>Process:</td><td>/bin/gzip</td></tr>
<tr><td>File Type:</td><td>gzip compressed data, last modified: Wed Oct 20 23:57:29 2021, from Unix</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>3073</td></tr>
<tr><td>Entropy (8bit):</td><td>7.943777100465176</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:v2e9EbH9DtolAKJARQAGwRRR2vJRWqKT2/R:+eWZqlAKJSQArEvJRWqKg</td></tr>
<tr><td>MD5:</td><td>235B747F3F9A90C66AB8605FAE6BA700</td></tr>
<tr><td>SHA1:</td><td>5F4E505268572CCF34B86F084B64956DF483C661</td></tr>
<tr><td>SHA-256:</td><td>7CFB8D6E0F4063BD4C7739FDD2D3BFBB24B8D604133C21A9BBCF50542EE0AD26</td></tr>
<tr><td>SHA-512:</td><td>2D030DCF8F4F785187828E2D050E6B27171A33E5D82A78E4313CCC04142C14DB1AC73A973A1B1A881C81214DBBB2B7B836D78596AB41F7AE37BFDEE4F0CCA48</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.....pa...\is...._...g;!...:.....Yo.d..d<..I.H.!@....R.e..u...Y.....CR +@f.......0.)F%....$}t..t.R..X.qI...7....R.....iZ...{.H...D.|..1.hS!.......n.,....9.....$...)xT.<......)......wiL.hX.1!.I.5...|J......h.f.+./..'\..g...0.F.H\....O2...`.3z.....4._..8.WY..p,.;.2A....+'..|.`.1.WEr...P.R.].e....P...g......"S.ND<M...D`..h.*qB...`...9..Nxo. i..1...o....N`..8.m6p.$.BI.Ez..<.P,*P_G...c5.k0.$`h>]...!...I.A.>.[.D1K.`..CHT|`.._.....wG.........x..t!.......$o.@..*...`.,.1gb.......p?..1.!.......i.@..,....F.Z.....j..<..`:.&ly.....-..*9H..XL....<.}..d.%..:~.R..T%..U)d._......rR..pA.c~..I....`.*...,.Z-I,X..E..'..4.h.#@...}.Z...5z.zf...o.. .'$..8......f..^....l3...%n......q}...{v...+..G....K..;.,..p...D.....\...W....[..?^...:4..6..;........#I.^..m..c..}|7....G.].3.(Rk..g.......s...q..x..t.#8..,G=.{=..G.4.....@.vd-...dJ....c...g.Q.)e.-.L.....=P..|......e .....j/.Vck[..5m..e..)...0..,...j.......w.q.n.s.e...2(....)..9A|Zb:Cb......O.G...&.2...1.t\._C</td></tr>
</table>

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.973187970686871
TrID:	- ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm
File size:	43984
MD5:	b03983514a53cfd40e45de31716bcd9e
SHA1:	77a0aeccab53179f50a8438e3ab416eda5ac6c06
SHA256:	171e2181f456498f53cc39fc7de35f1f10d40c026d3a9b74b88618b9402dcf30
SHA512:	d64d56d90ed8d07266901dbf78844b533d523ceb4c4500778543068b7896d76a3166bc6fb00115bccfc11881567124ffd5290851963363037a587b3b95305ea
SSDEEP:	768:eDpn0egnpPn1A7TNDRaT30QkjmaiV/3WKoQPyJvWXinefVB9JfLss3Uoz3:eDyegpv12TNDwD0QkjXiRPoQqtCfVB9/

General

File Content Preview:	.ELF...a..........(.....(...4...........4. ...(..y..........................Q.td................................UPX!........x...x.......S..........?.E.h;.}...^..........fQ.>..??tJ_BA.s3.n..N..N.+x^.....X.z..d..<.H..

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x11928
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0xaad7	0xaad7	4.0246	0x5	R E	0x8000		
LOAD	0x7900	0x2f900	0x2f900	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 21, 2021 01:58:56.824167013 CEST	192.168.2.23	1.1.1.1	0xd850	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Oct 21, 2021 01:58:56.824203968 CEST	192.168.2.23	1.1.1.1	0xeba5	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Oct 21, 2021 01:58:56.938555956 CEST	192.168.2.23	1.1.1.1	0xe2b7	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 01:58:56.840388060 CEST	1.1.1.1	192.168.2.23	0xd850	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Oct 21, 2021 01:58:56.840388060 CEST	1.1.1.1	192.168.2.23	0xd850	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: systemd PID: 5213 Parent PID: 1

General

Start time:	01:57:54
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5213 Parent PID: 1

General

Start time:	01:57:54
Start date:	21/10/2021
Path:	/usr/sbin/logrotate
Arguments:	/usr/sbin/logrotate /etc/logrotate.conf
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: logrotate PID: 5311 Parent PID: 5213

General

Start time:	01:57:55
Start date:	21/10/2021
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5311 Parent PID: 5213

General

Start time:	01:57:55
Start date:	21/10/2021

Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5312 Parent PID: 5213

General

Start time:	01:57:55
Start date:	21/10/2021
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5312 Parent PID: 5213

General

Start time:	01:57:55
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5313 Parent PID: 5312

General

Start time:	01:57:55
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5313 Parent PID: 5312

General

Start time:	01:57:55
Start date:	21/10/2021

Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: invoke-rc.d PID: 5314 Parent PID: 5313

General

Start time:	01:57:56
Start date:	21/10/2021
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: runlevel PID: 5314 Parent PID: 5313

General

Start time:	01:57:56
Start date:	21/10/2021
Path:	/sbin/runlevel
Arguments:	/sbin/runlevel
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5315 Parent PID: 5313

General

Start time:	01:57:56
Start date:	21/10/2021
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5315 Parent PID: 5313

General

Start time:	01:57:56
Start date:	21/10/2021

Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-enabled cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5320 Parent PID: 5313

General

Start time:	01:57:57
Start date:	21/10/2021
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: ls PID: 5320 Parent PID: 5313

General

Start time:	01:57:57
Start date:	21/10/2021
Path:	/usr/bin/ls
Arguments:	ls /etc/rc[S2345].d/S[0-9][0-9]cups
File size:	142144 bytes
MD5 hash:	e7793f15c2ff7e747b4bc7079f5cd4f7

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5321 Parent PID: 5313

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5321 Parent PID: 5313

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active cups.service
File size:	996584 bytes

MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: logrotate PID: 5322 Parent PID: 5213

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5322 Parent PID: 5213

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5323 Parent PID: 5213

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5323 Parent PID: 5213

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5324 Parent PID: 5323

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: 5324 Parent PID: 5323

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	/usr/lib/rsyslog/rsyslog-rotate
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: rsyslog-rotate PID: 5325 Parent PID: 5324

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5325 Parent PID: 5324

General

Start time:	01:57:58
Start date:	21/10/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl kill -s HUP rsyslog.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: systemd PID: 5218 Parent PID: 1

General

Start time:	01:57:54
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: 5218 Parent PID: 1

General

Start time:	01:57:54
Start date:	21/10/2021
Path:	/usr/bin/install
Arguments:	/usr/bin/install -d -o man -g man -m 0755 /var/cache/man
File size:	158112 bytes
MD5 hash:	55e2520049dc6a62e8c94732e36cdd54

File Activities

File Read

Directory Created

Analysis Process: systemd PID: 5297 Parent PID: 1

General

Start time:	01:57:54
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: 5297 Parent PID: 1

General

Start time:	01:57:54
Start date:	21/10/2021
Path:	/usr/bin/find
Arguments:	/usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
File size:	320160 bytes
MD5 hash:	b68ef002f84cc54dd472238ba7df80ab

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5316 Parent PID: 1

General

Start time:	01:57:56
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: 5316 Parent PID: 1

General

Start time:	01:57:56
Start date:	21/10/2021
Path:	/usr/bin/mandb
Arguments:	/usr/bin/mandb --quiet
File size:	142432 bytes
MD5 hash:	1dda5ea0027ecf1c2db0f5a3de7e6941

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: arm PID: 5339 Parent PID: 5121

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	/tmp/arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: arm PID: 5341 Parent PID: 5339

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5342 Parent PID: 5339

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5344 Parent PID: 5339

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5345 Parent PID: 5339

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5348 Parent PID: 5339

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5352 Parent PID: 5339

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5355 Parent PID: 5352

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: arm PID: 5357 Parent PID: 5352

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm PID: 5359 Parent PID: 5357

General

Start time:	01:58:10
Start date:	21/10/2021
Path:	/tmp/arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5402 Parent PID: 1

General

Start time:	01:58:55
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5402 Parent PID: 1

General

Start time:	01:58:55
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: 5425 Parent PID: 1

General

Start time:	01:59:00
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5425 Parent PID: 1

General

Start time:	01:59:00
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: 5426 Parent PID: 1

General

Start time:	01:59:00
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5426 Parent PID: 1

General

Start time:	01:59:00
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: 5429 Parent PID: 1320

General

Start time:	01:59:06
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5429 Parent PID: 1320

General

Start time:	01:59:06
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: 5434 Parent PID: 1320

General

Start time:	01:59:06
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5434 Parent PID: 1320

General

Start time:	01:59:06
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: 5435 Parent PID: 1

General

Start time:	01:59:07
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: 5435 Parent PID: 1

General

Start time:	01:59:07
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: 5452 Parent PID: 5435

General

Start time:	01:59:07
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: 5452 Parent PID: 5435

General

Start time:	01:59:07
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: 5453 Parent PID: 5452

General

Start time:	01:59:07
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: 5453 Parent PID: 5452

General

Start time:	01:59:07
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: 5454 Parent PID: 5453

General

Start time:	01:59:07
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: 5454 Parent PID: 5453

General

Start time:	01:59:07
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: 5455 Parent PID: 5454

General

Start time:	01:59:07
Start date:	21/10/2021
Path:	/bin/sh

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

Analysis Process: locale PID: 5455 Parent PID: 5454

General

Start time:	01:59:07
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: 5456 Parent PID: 5454

General

Start time:	01:59:07
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5456 Parent PID: 5454

General

Start time:	01:59:07
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: 5457 Parent PID: 1320

General

Start time:	01:59:08
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: 5457 Parent PID: 1320

General

Start time:	01:59:08
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: 5461 Parent PID: 5457

General

Start time:	01:59:10
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: 5461 Parent PID: 5457

General

Start time:	01:59:10
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: 5464 Parent PID: 5461

General

Start time:	01:59:10

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: 5464 Parent PID: 5461

General

Start time:	01:59:10
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: 5465 Parent PID: 5464

General

Start time:	01:59:11
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: 5465 Parent PID: 5464

General

Start time:	01:59:11
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: 5471 Parent PID: 5465

General

Start time:	01:59:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5472 Parent PID: 5471

General

Start time:	01:59:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5472 Parent PID: 5471

General

Start time:	01:59:12
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: 5474 Parent PID: 5465

General

Start time:	01:59:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5475 Parent PID: 5474

General

Start time:	01:59:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5475 Parent PID: 5474

General

Start time:	01:59:12
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: 5476 Parent PID: 5465

General

Start time:	01:59:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5477 Parent PID: 5476

General

Start time:	01:59:12
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5477 Parent PID: 5476

General

Start time:	01:59:12
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: 5478 Parent PID: 5465

General

Start time:	01:59:13
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: 5479 Parent PID: 5478

General

Start time:	01:59:13
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: 5479 Parent PID: 5478

General

Start time:	01:59:13
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5480 Parent PID: 5465

General

Start time:	01:59:13
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: 5481 Parent PID: 5480

General

Start time:	01:59:13
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: 5481 Parent PID: 5480

General

Start time:	01:59:13
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5482 Parent PID: 5465

General

Start time:	01:59:13
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: 5483 Parent PID: 5482

General

Start time:	01:59:13
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: 5483 Parent PID: 5482

General

Start time:	01:59:13
Start date:	21/10/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5485 Parent PID: 5465

General

Start time:	01:59:14
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: 5486 Parent PID: 5485

General

Start time:	01:59:14
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: 5486 Parent PID: 5485

General

Start time:	01:59:14
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: 5466 Parent PID: 5464

General

Start time:	01:59:11
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: 5466 Parent PID: 5464

General

Start time:	01:59:11
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: 5466 Parent PID: 5464

General

Start time:	01:59:11
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: 5487 Parent PID: 5466

General

Start time:	01:59:14
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: 5487 Parent PID: 5466

General

Start time:	01:59:14
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: 5488 Parent PID: 5466

General

Start time:	01:59:14
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: 5488 Parent PID: 5466

General

Start time:	01:59:14
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: 5488 Parent PID: 5466

General

Start time:	01:59:15
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: 5496 Parent PID: 1320

General

Start time:	01:59:18
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: 5496 Parent PID: 1320

General

Start time:	01:59:18
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: 5523 Parent PID: 5496

General

Start time:	01:59:20
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: 5523 Parent PID: 5496

General

Start time:	01:59:20
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: 5525 Parent PID: 5523

General

Start time:	01:59:20
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: 5525 Parent PID: 5523

General

Start time:	01:59:20
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: 5525 Parent PID: 5523

General

Start time:	01:59:20
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: 5525 Parent PID: 5523

General

Start time:	01:59:21
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: 5553 Parent PID: 5525

General

Start time:	01:59:30
Start date:	21/10/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5553 Parent PID: 5525

General

Start time:	01:59:30
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: 5554 Parent PID: 5553

General

Start time:	01:59:31
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5554 Parent PID: 5553

General

Start time:	01:59:31
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: 5986 Parent PID: 5525

General

Start time:	02:00:12
Start date:	21/10/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5986 Parent PID: 5525

General

Start time:	02:00:12
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5987 Parent PID: 5986

General

Start time:	02:00:13
Start date:	21/10/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5987 Parent PID: 5986

General

Start time:	02:00:13
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: 5567 Parent PID: 5523

General

Start time:	01:59:38
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: 5567 Parent PID: 5523

General

Start time:	01:59:38
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: 5568 Parent PID: 5523

General

Start time:	01:59:38
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: 5568 Parent PID: 5523

General

Start time:	01:59:38
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: 5569 Parent PID: 5568

General

Start time:	01:59:38
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: 5569 Parent PID: 5568

General

Start time:	01:59:38
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: 5631 Parent PID: 5569

General

Start time:	01:59:49
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: 5632 Parent PID: 5631

General

Start time:	01:59:49
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: 5632 Parent PID: 5631

General

Start time:	01:59:49
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: 5637 Parent PID: 5632

General

Start time:	01:59:50
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: 5637 Parent PID: 5632

General

Start time:	01:59:50
Start date:	21/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5994 Parent PID: 5637

General

Start time:	02:00:16
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: 5995 Parent PID: 5994

General

Start time:	02:00:16
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: 5995 Parent PID: 5994

General

Start time:	02:00:17
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: 5661 Parent PID: 5569

General

Start time:	01:59:53
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: 5662 Parent PID: 5661

General

Start time:	01:59:53
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: 5662 Parent PID: 5661

General

Start time:	01:59:53
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: 5664 Parent PID: 5569

General

Start time:	01:59:53
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: 5665 Parent PID: 5664

General

Start time:	01:59:53
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: 5665 Parent PID: 5664

General

Start time:	01:59:53
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: 5666 Parent PID: 5569

General

Start time:	01:59:53
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: 5667 Parent PID: 5666

General

Start time:	01:59:53
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: 5667 Parent PID: 5666

General

Start time:	01:59:54
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: 5668 Parent PID: 5569

General

Start time:	01:59:55
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: 5669 Parent PID: 5668

General

Start time:	01:59:55
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: 5669 Parent PID: 5668

General

Start time:	01:59:55
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: 5670 Parent PID: 5569

General

Start time:	01:59:55
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: 5671 Parent PID: 5670

General

Start time:	01:59:55
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: 5671 Parent PID: 5670

General

Start time:	01:59:55
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: 5672 Parent PID: 5569

General

Start time:	01:59:55
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: 5673 Parent PID: 5672

General

Start time:	01:59:55
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: 5673 Parent PID: 5672

General

Start time:	01:59:55
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: 5675 Parent PID: 5569

General

Start time:	01:59:55
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: 5676 Parent PID: 5675

General

Start time:	01:59:55
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: 5676 Parent PID: 5675

General

Start time:	01:59:55
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: 5979 Parent PID: 5569

General

Start time:	02:00:11
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: 5980 Parent PID: 5979

General

Start time:	02:00:11
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: 5980 Parent PID: 5979

General

Start time:	02:00:11
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: 6207 Parent PID: 5569

General

Start time:	02:00:19
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: 6208 Parent PID: 6207

General

Start time:	02:00:19
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: 6208 Parent PID: 6207

General

Start time:	02:00:19
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: 6276 Parent PID: 5569

General

Start time:	02:00:36
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: 6277 Parent PID: 6276

General

Start time:	02:00:36
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: 6277 Parent PID: 6276

General

Start time:	02:00:36
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: 5570 Parent PID: 5568

General

Start time:	01:59:38
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: 5570 Parent PID: 5568

General

Start time:	01:59:38
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: 5570 Parent PID: 5568

General

Start time:	01:59:38
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: 5571 Parent PID: 5570

General

Start time:	01:59:39
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: 5571 Parent PID: 5570

General

Start time:	01:59:39
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: 5638 Parent PID: 5571

General

Start time:	01:59:51
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: 5638 Parent PID: 5571

General

Start time:	01:59:51
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: 5648 Parent PID: 5571

General

Start time:	01:59:51
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: 5648 Parent PID: 5571

General

Start time:	01:59:51
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: 5677 Parent PID: 5570

General

Start time:	01:59:55
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: 5677 Parent PID: 5570

General

Start time:	01:59:55
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: 5678 Parent PID: 5570

General

Start time:	01:59:56
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: 5678 Parent PID: 5570

General

Start time:	01:59:56
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: 5678 Parent PID: 5570

General

Start time:	01:59:56
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: 5784 Parent PID: 5678

General

Start time:	02:00:10
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: 5784 Parent PID: 5678

General

Start time:	02:00:10
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: 5908 Parent PID: 5784

General

Start time:	02:00:11
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: 5908 Parent PID: 5784

General

Start time:	02:00:11
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: 5939 Parent PID: 5784

General

Start time:	02:00:11
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: 5942 Parent PID: 5939

General

Start time:	02:00:11
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: 5942 Parent PID: 1

General

Start time:	02:00:11
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: 6251 Parent PID: 5784

General

Start time:	02:00:27

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: 6251 Parent PID: 5784

General

Start time:	02:00:27
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: 6228 Parent PID: 5570

General

Start time:	02:00:23
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: 6228 Parent PID: 5570

General

Start time:	02:00:23
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: 6228 Parent PID: 5570

General

Start time:	02:00:23
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: 6230 Parent PID: 5570

General

Start time:	02:00:23
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: 6230 Parent PID: 5570

General

Start time:	02:00:23
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: 6230 Parent PID: 5570

General

Start time:	02:00:23
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: 6232 Parent PID: 5570

General

Start time:	02:00:23
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: 6232 Parent PID: 5570

General

Start time:	02:00:23
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

Analysis Process: gsd-color PID: 6232 Parent PID: 5570

General

Start time:	02:00:23
Start date:	21/10/2021
Path:	/usr/libexec/gsd-color
Arguments:	/usr/libexec/gsd-color
File size:	92832 bytes
MD5 hash:	ac2861ad93ce047283e8e87cefef9a19

Analysis Process: gnome-session-binary PID: 6233 Parent PID: 5570

General

Start time:	02:00:23

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: 6233 Parent PID: 5570

General

Start time:	02:00:23
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

Analysis Process: gsd-keyboard PID: 6233 Parent PID: 5570

General

Start time:	02:00:23
Start date:	21/10/2021
Path:	/usr/libexec/gsd-keyboard
Arguments:	/usr/libexec/gsd-keyboard
File size:	39760 bytes
MD5 hash:	8e288fd17c80bb0a1148b964b2ac2279

Analysis Process: gnome-session-binary PID: 6234 Parent PID: 5570

General

Start time:	02:00:23
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: 6234 Parent PID: 5570

General

Start time:	02:00:23
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

Analysis Process: gsd-print-notifications PID: 6234 Parent PID: 5570

General

Start time:	02:00:25
Start date:	21/10/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6554 Parent PID: 6234

General

Start time:	02:00:38
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: 6555 Parent PID: 6554

General

Start time:	02:00:38
Start date:	21/10/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-printer PID: 6555 Parent PID: 1

General

Start time:	02:00:38
Start date:	21/10/2021
Path:	/usr/libexec/gsd-printer
Arguments:	/usr/libexec/gsd-printer
File size:	31120 bytes
MD5 hash:	7995828cf98c315fd55f2ffb3b22384d

Analysis Process: gnome-session-binary PID: 6235 Parent PID: 5570

General

Start time:	02:00:24
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: 6235 Parent PID: 5570

General

Start time:	02:00:25
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

Analysis Process: gsd-rfkill PID: 6235 Parent PID: 5570

General

Start time:	02:00:25
Start date:	21/10/2021
Path:	/usr/libexec/gsd-rfkill
Arguments:	/usr/libexec/gsd-rfkill
File size:	51808 bytes
MD5 hash:	88a16a3c0aba1759358c06215ecfb5cc

Analysis Process: gnome-session-binary PID: 6236 Parent PID: 5570

General

Start time:	02:00:25
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: 6236 Parent PID: 5570

General

Start time:	02:00:25
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

Analysis Process: gsd-smartcard PID: 6236 Parent PID: 5570

General

Start time:	02:00:25
Start date:	21/10/2021
Path:	/usr/libexec/gsd-smartcard
Arguments:	/usr/libexec/gsd-smartcard
File size:	109152 bytes
MD5 hash:	ea1fbd7f62e4cd0331eae2ef754ee605

Analysis Process: gnome-session-binary PID: 6238 Parent PID: 5570

General

Start time:	02:00:25
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: 6238 Parent PID: 5570

General

Start time:	02:00:25
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

Analysis Process: gsd-datetime PID: 6238 Parent PID: 5570

General

Start time:	02:00:25
Start date:	21/10/2021
Path:	/usr/libexec/gsd-datetime
Arguments:	/usr/libexec/gsd-datetime
File size:	76736 bytes
MD5 hash:	d80d39745740de37d6634d36e344d4bc

Analysis Process: gnome-session-binary PID: 6239 Parent PID: 5570

General

Start time:	02:00:25
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: 6239 Parent PID: 5570

General

Start time:	02:00:25
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

Analysis Process: gsd-media-keys PID: 6239 Parent PID: 5570

General

Start time:	02:00:25
Start date:	21/10/2021
Path:	/usr/libexec/gsd-media-keys
Arguments:	/usr/libexec/gsd-media-keys
File size:	232936 bytes
MD5 hash:	a425448c135afb4b8bfd79cc0b6b74da

Analysis Process: gnome-session-binary PID: 6240 Parent PID: 5570

General

Start time:	02:00:25
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: 6240 Parent PID: 5570

General

Start time:	02:00:25
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

Analysis Process: gsd-screensaver-proxy PID: 6240 Parent PID: 5570

General

Start time:	02:00:27
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: 6241 Parent PID: 5570

General

Start time:	02:00:26
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: 6241 Parent PID: 5570

General

Start time:	02:00:27
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: 6241 Parent PID: 5570

General

Start time:	02:00:27
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: 6248 Parent PID: 5570

General

Start time:	02:00:27
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: 6248 Parent PID: 5570

General

Start time:	02:00:27
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: 6248 Parent PID: 5570

General

Start time:	02:00:27
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: 6249 Parent PID: 5570

General

Start time:	02:00:27
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: 6249 Parent PID: 5570

General

Start time:	02:00:27
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: 6249 Parent PID: 5570

General

Start time:	02:00:29
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: 6254 Parent PID: 5570

General

Start time:	02:00:27
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: 6254 Parent PID: 5570

General

Start time:	02:00:29
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: 6254 Parent PID: 5570

General

Start time:	02:00:29
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: 7121 Parent PID: 5570

General

Start time:	02:01:06
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: 7121 Parent PID: 5570

General

Start time:	02:01:06
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: 7121 Parent PID: 5570

General

Start time:	02:01:06
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: 7125 Parent PID: 5570

General

Start time:	02:01:08

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: 7125 Parent PID: 5570

General

Start time:	02:01:08
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: 7125 Parent PID: 5570

General

Start time:	02:01:09
Start date:	21/10/2021
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5513 Parent PID: 1320

General

Start time:	01:59:18
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5513 Parent PID: 1320

General

Start time:	01:59:18
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: 5518 Parent PID: 1320

General

Start time:	01:59:18
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5518 Parent PID: 1320

General

Start time:	01:59:18
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: 5528 Parent PID: 1320

General

Start time:	01:59:24
Start date:	21/10/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5528 Parent PID: 1320

General

Start time:	01:59:24
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: 5533 Parent PID: 1860

General

Start time:	01:59:28
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5533 Parent PID: 1860

General

Start time:	01:59:28
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: 5572 Parent PID: 2038

General

Start time:	01:59:40
Start date:	21/10/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5572 Parent PID: 2038

General

Start time:	01:59:40
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: 5595 Parent PID: 1

General

Start time:	01:59:42
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: 5595 Parent PID: 1

General

Start time:	01:59:42
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: 5703 Parent PID: 1

General

Start time:	02:00:11
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: 5703 Parent PID: 1

General

Start time:	02:00:11
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: 5991 Parent PID: 1334

General

Start time:	02:00:14
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5991 Parent PID: 1334

General

Start time:	02:00:14
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: 5996 Parent PID: 1

General

Start time:	02:00:17
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5996 Parent PID: 1

General

Start time:	02:00:17
Start date:	21/10/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 6278 Parent PID: 1

General

Start time:	02:00:37
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: 6278 Parent PID: 1

General

Start time:	02:00:37
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: 6652 Parent PID: 1

General

Start time:	02:01:02
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: 6652 Parent PID: 1

General

Start time:	02:01:02
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: 6684 Parent PID: 1

General

Start time:	02:01:02
Start date:	21/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6684 Parent PID: 1

General

Start time:	02:01:02
Start date:	21/10/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84