ID: 512564
Sample Name: HgTC70XRum
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:51:12
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

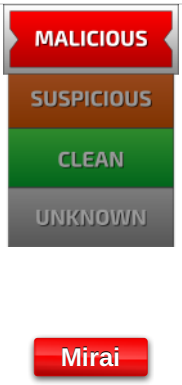
Linux Analysis Report HgTC70XRum

Overview

General Information

Sample Name:	HgTC70XRum
Analysis ID:	512564
MD5:	511762f1b10eab0.
SHA1:	f51d425c38135a2.
SHA256:	19818befeeaaa5b.
Tags:	32 elf mirai motorola
Infos:	

Detection

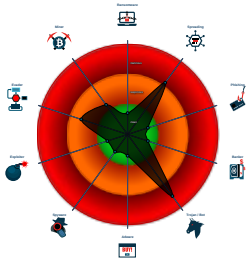


Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample tries to kill many processes...
- Connects to many ports of the same...
- Reads system files that contain reco...
- Uses known network protocols on no...
- Sample reads /proc/mounts (often u...
- Reads CPU information from /sys in...
- Yara signature match
- Executes the "grep" command used...
- Uses the "uname" system call to qu...

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512564
Start date:	01.11.2021
Start time:	04:51:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HgTC70XRum
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal84.spre.troj.lin@0/111@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- HgTC70XRum (PID: 5247, Parent: 5118, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/HgTC70XRum
  - HgTC70XRum New Fork (PID: 5249, Parent: 5247)
    - HgTC70XRum New Fork (PID: 5251, Parent: 5249)
    - HgTC70XRum New Fork (PID: 5252, Parent: 5249)
    - HgTC70XRum New Fork (PID: 5255, Parent: 5249)
    - HgTC70XRum New Fork (PID: 5258, Parent: 5249)
    - HgTC70XRum New Fork (PID: 5259, Parent: 5249)
    - HgTC70XRum New Fork (PID: 5262, Parent: 5249)

- HgTC70XRum New Fork (PID: 5263, Parent: 5249)
- HgTC70XRum New Fork (PID: 5265, Parent: 5249)

- systemd New Fork (PID: 5276, Parent: 1)
- sshd (PID: 5276, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5277, Parent: 1)
- sshd (PID: 5277, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5292, Parent: 1)
- systemd-resolved (PID: 5292, Parent: 1, MD5: c93bbc5e20248114c56896451eab7a8b) Arguments: /lib/systemd/systemd-resolved
- systemd New Fork (PID: 5574, Parent: 1)
- systemd-logind (PID: 5574, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5709, Parent: 1)
- accounts-daemon (PID: 5709, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5724, Parent: 5709)
  - language-validate (PID: 5724, Parent: 5709, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5725, Parent: 5724)
    - language-options (PID: 5725, Parent: 5724, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5726, Parent: 5725)
      - sh (PID: 5726, Parent: 5725, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5727, Parent: 5726)
        - locale (PID: 5727, Parent: 5726, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5728, Parent: 5726)
        - grep (PID: 5728, Parent: 5726, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- xfce4-session New Fork (PID: 5712, Parent: 1900)
- systemd New Fork (PID: 5715, Parent: 1860)
- pulseaudio (PID: 5715, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gdm-session-worker New Fork (PID: 5721, Parent: 1809)
- Default (PID: 5721, Parent: 1809, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PostSession/Default
- gdm3 New Fork (PID: 5733, Parent: 1320)
- gdm-session-worker (PID: 5733, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5740, Parent: 5733)
  - gdm-x-session (PID: 5740, Parent: 5733, 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: 5742, Parent: 5740)
    - Xorg (PID: 5742, Parent: 5740, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg.wrap (PID: 5742, Parent: 5740, MD5: 48993830888200ecf19dd7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg (PID: 5742, Parent: 5740, MD5: 730cf4c45a7ee8bea88abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg New Fork (PID: 5753, Parent: 5742)
      - sh (PID: 5753, Parent: 5742, 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: 5754, Parent: 5753)
        - xkbcomp (PID: 5754, Parent: 5753, 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: 5774, Parent: 5740)
    - dbus-daemon (PID: 5774, Parent: 5740, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 4 --session
      - dbus-daemon New Fork (PID: 5778, Parent: 5774)
        - dbus-daemon New Fork (PID: 5779, Parent: 5778)
        - false (PID: 5779, Parent: 5778, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- gdm3 New Fork (PID: 5736, Parent: 1320)
- Default (PID: 5736, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5737, Parent: 1320)
- Default (PID: 5737, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5738, Parent: 1320)
- Default (PID: 5738, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5780, Parent: 1320)
- Default (PID: 5780, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5781, Parent: 1320)
- Default (PID: 5781, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5828, Parent: 1)
- sshd (PID: 5828, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5831, Parent: 1)
- systemd-resolved (PID: 5831, Parent: 1, MD5: c93bbc5e20248114c56896451eab7a8b) Arguments: /lib/systemd/systemd-resolved
- systemd New Fork (PID: 5847, Parent: 1)
- sshd (PID: 5847, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 6095, Parent: 1)
- systemd-logind (PID: 6095, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 6214, Parent: 1)
- accounts-daemon (PID: 6214, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 6220, Parent: 6214)
  - language-validate (PID: 6220, Parent: 6214, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 6221, Parent: 6220)
    - language-options (PID: 6221, Parent: 6220, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 6222, Parent: 6221)
      - sh (PID: 6222, Parent: 6221, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 6223, Parent: 6222)
        - locale (PID: 6223, Parent: 6222, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 6224, Parent: 6222)
        - grep (PID: 6224, Parent: 6222, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm3 New Fork (PID: 6225, Parent: 1320)
- gdm-session-worker (PID: 6225, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 6240, Parent: 6225)
  - gdm-x-session (PID: 6240, Parent: 6225, 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: 6242, Parent: 6240)
    - Xorg (PID: 6242, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg.wrap (PID: 6242, Parent: 6240, MD5: 48993830888200ecf19dd7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3

- Xorg (PID: 6242, Parent: 6240, MD5: 730cf4c45a7ee8bea88abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
  - Xorg New Fork (PID: 6429, Parent: 6242)
  - sh (PID: 6429, Parent: 6242, 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: 6506, Parent: 6429)
    - xkbcomp (PID: 6506, Parent: 6429, 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: 6678, Parent: 6240)
- dbus-daemon (PID: 6678, Parent: 6240, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 4 --session
  - dbus-daemon New Fork (PID: 6680, Parent: 6678)
    - dbus-daemon New Fork (PID: 6681, Parent: 6680)
    - false (PID: 6681, Parent: 6680, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false

- systemd New Fork (PID: 6231, Parent: 1)
- systemd (PID: 6231, Parent: 1, MD5: 9b2bec7092a40488108543f9334aab75) Arguments: /lib/systemd/systemd --user
  - systemd New Fork (PID: 6243, Parent: 6231)
    - systemd New Fork (PID: 6244, Parent: 6243)
    - 30-systemd-environment-d-generator (PID: 6244, Parent: 6243, MD5: 42417da8051ba8ee0eea7854c62d99ca) Arguments: /usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
  - systemd New Fork (PID: 6251, Parent: 6231)
  - systemctl (PID: 6251, Parent: 6231, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
  - systemd New Fork (PID: 6252, Parent: 6231)
  - pulseaudio (PID: 6252, Parent: 6231, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 6267, Parent: 1)
- systemd-resolved (PID: 6267, Parent: 1, MD5: c93bbc5e20248114c56896451eab7a8b) Arguments: /lib/systemd/systemd-resolved
- systemd New Fork (PID: 6552, Parent: 1)
- sshd (PID: 6552, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 6555, Parent: 1)
- systemd-logind (PID: 6555, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 6672, Parent: 1)
- sshd (PID: 6672, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 6675, Parent: 1320)
- Default (PID: 6675, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 6676, Parent: 1320)
- Default (PID: 6676, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 6690, Parent: 1)
- systemd-resolved (PID: 6690, Parent: 1, MD5: c93bbc5e20248114c56896451eab7a8b) Arguments: /lib/systemd/systemd-resolved
- systemd New Fork (PID: 6953, Parent: 1)
- systemd-logind (PID: 6953, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 7072, Parent: 1)
- agetty (PID: 7072, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\u" --noclear tty2 linux
- systemd New Fork (PID: 7073, Parent: 1)
- accounts-daemon (PID: 7073, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 7078, Parent: 7073)
  - language-validate (PID: 7078, Parent: 7073, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 7079, Parent: 7078)
    - language-options (PID: 7079, Parent: 7078, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 7080, Parent: 7079)
      - sh (PID: 7080, Parent: 7079, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 7081, Parent: 7080)
        - locale (PID: 7081, Parent: 7080, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 7083, Parent: 7080)
        - grep (PID: 7083, Parent: 7080, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 7077, Parent: 1)
- sshd (PID: 7077, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 7082, Parent: 1)
- sshd (PID: 7082, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 7084, Parent: 1320)
- gdm-session-worker (PID: 7084, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 7092, Parent: 7084)
  - gdm-x-session (PID: 7092, Parent: 7084, 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: 7095, Parent: 7092)
    - Xorg (PID: 7095, Parent: 7092, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt3 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg.wrap (PID: 7095, Parent: 7092, MD5: 48993830888200ecf19dd7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt3 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg (PID: 7095, Parent: 7092, MD5: 730cf4c45a7ee8bea88abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt3 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg New Fork (PID: 7497, Parent: 7095)
      - sh (PID: 7497, Parent: 7095, 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: 7498, Parent: 7497)
        - xkbcomp (PID: 7498, Parent: 7497, 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: 7500, Parent: 7092)
    - dbus-daemon (PID: 7500, Parent: 7092, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 4 --session
      - dbus-daemon New Fork (PID: 7502, Parent: 7500)
        - dbus-daemon New Fork (PID: 7503, Parent: 7502)
        - false (PID: 7503, Parent: 7502, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- systemd New Fork (PID: 7088, Parent: 1)
- systemd (PID: 7088, Parent: 1, MD5: 9b2bec7092a40488108543f9334aab75) Arguments: /lib/systemd/systemd --user
  - systemd New Fork (PID: 7094, Parent: 7088)
    - systemd New Fork (PID: 7096, Parent: 7094)
    - 30-systemd-environment-d-generator (PID: 7096, Parent: 7094, MD5: 42417da8051ba8ee0eea7854c62d99ca) Arguments: /usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
  - systemd New Fork (PID: 7483, Parent: 7088)
  - systemctl (PID: 7483, Parent: 7088, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus

- systemd New Fork (PID: 7486, Parent: 7088)
  - pulseaudio (PID: 7486, Parent: 7088, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 7101, Parent: 1)
  - systemd-resolved (PID: 7101, Parent: 1, MD5: c93bbc5e20248114c56896451eab7a8b) Arguments: /lib/systemd/systemd-resolved
- systemd New Fork (PID: 7366, Parent: 1)
  - systemd-logind (PID: 7366, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 7484, Parent: 1)
  - sshd (PID: 7484, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 7485, Parent: 1)
  - sshd (PID: 7485, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 7489, Parent: 1320)
  - Default (PID: 7489, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 7490, Parent: 1320)
  - Default (PID: 7490, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- **cleanup**

Yara Overview

Initial Sample

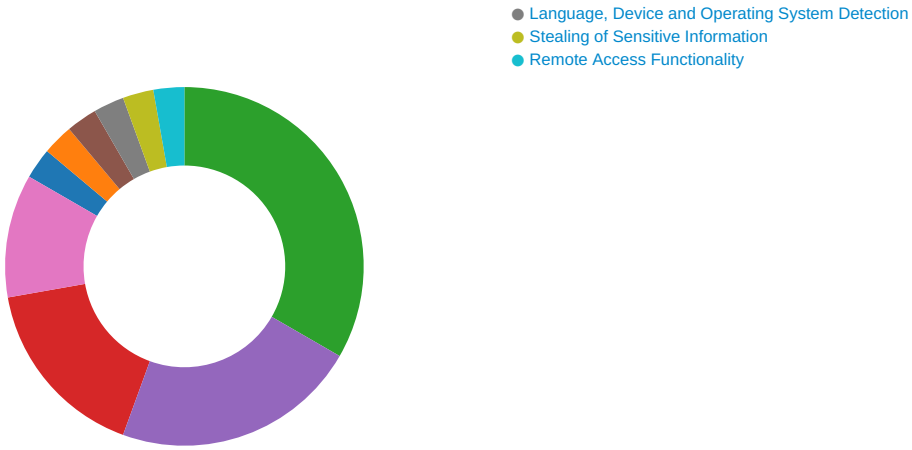
Source	Rule	Description	Author	Strings
HgTC70XRum	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x114af:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1150b:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x115a6:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
HgTC70XRum	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5255.1.000000007179dd3c.0000000045078886.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x128c:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x12ec:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1390:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
5251.1.00000000aea00156.000000007179dd3c.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x4af:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x50b:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x5a6:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
5252.1.0000000058a0b464.00000000661e3bb3.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x114af:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1150b:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x115a6:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
5252.1.0000000058a0b464.00000000661e3bb3.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5259.1.000000007179dd3c.0000000045078886.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x128c:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x12ec:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1390:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
Click to see the 27 entries				

Jbx Signature Overview

- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

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

Uses known network protocols on non-standard ports

System Summary:

Sample tries to kill many processes (SIGKILL)

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

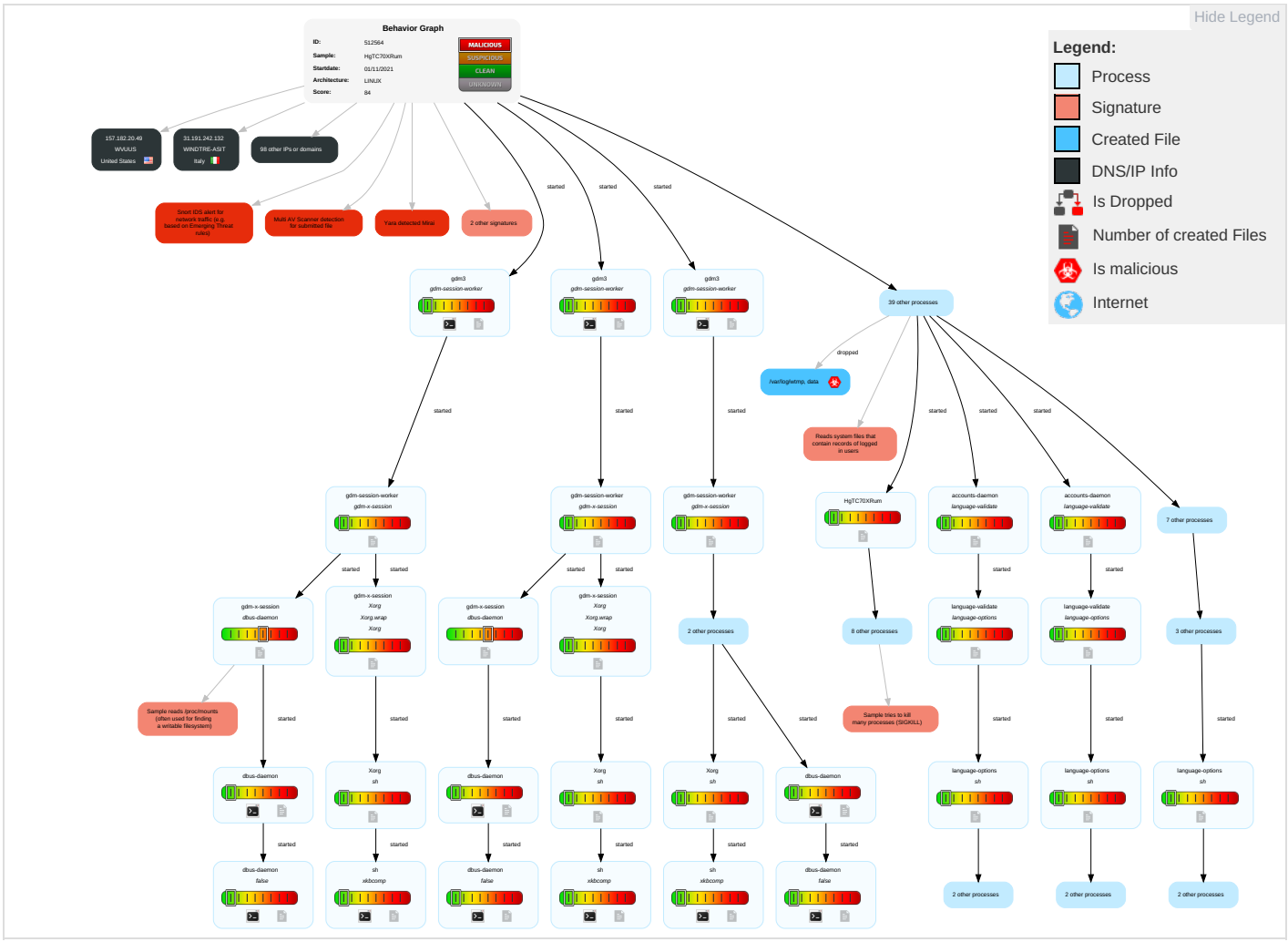
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Systemd Service 1	Systemd Service 1	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	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Indicator Removal on Host 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 4	Manipulate Device Communication		Manipu App Sto Rankin or Ratir

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HgTC70XRum	49%	Virustotal		Browse
HgTC70XRum	51%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:80/tmUnblock.cgi	0%	Virustotal		Browse
http://127.0.0.1:80/tmUnblock.cgi	0%	Avira URL Cloud	safe	
http://23.94.37.59/bin	0%	Avira URL Cloud	safe	
http://23.94.37.59/bins/Tsunami.mips;	100%	Avira URL Cloud	malware	
http://23.94.37.59/bins/Tsunami.x86	12%	Virustotal		Browse
http://23.94.37.59/bins/Tsunami.x86	100%	Avira URL Cloud	malware	
http://23.94.37.59/zyxel.sh;	0%	Avira URL Cloud	safe	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/tmUnblock.cgi	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.143.199.247	unknown	Russian Federation		57010	CLODO-ASRU	false
42.86.205.9	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
94.70.69.92	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
172.15.61.142	unknown	United States		7018	ATT-INTERNET4US	false
112.156.19.179	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
31.186.168.25	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
31.85.14.94	unknown	United Kingdom		12576	EELtdGB	false
197.86.54.125	unknown	South Africa		10474	OPTINETZA	false
98.123.237.122	unknown	United States		10796	TWC-10796-MIDWESTUS	false
172.197.166.141	unknown	Australia		18747	IFX18747US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.150.130.143	unknown	United States		7018	ATT-INTERNET4US	false
184.151.118.125	unknown	Canada		36522	BELLMOBILITY-1CA	false
31.136.150.35	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
157.182.20.49	unknown	United States		12118	WVUUS	false
112.97.88.167	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
210.125.75.11	unknown	Korea Republic of		9949	HOSEO-ASHoseoUniversityKR	false
172.147.85.230	unknown	United States		7018	ATT-INTERNET4US	false
95.106.122.231	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
94.52.101.0	unknown	Romania		48161	NG-ASSosBucuresti-Ploiestinr42-44RO	false
98.117.26.126	unknown	United States		701	UUNETUS	false
95.6.137.29	unknown	Turkey		9121	TTNETTR	false
172.147.112.193	unknown	United States		7018	ATT-INTERNET4US	false
98.142.17.46	unknown	United States		22402	NEXTCO-ASUS	false
98.48.231.148	unknown	United States		7922	COMCAST-7922US	false
85.230.40.164	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
85.146.193.172	unknown	Netherlands		33915	TNF-ASNL	false
172.227.134.124	unknown	United States		20940	AKAMAI-ASN1EU	false
172.147.112.196	unknown	United States		7018	ATT-INTERNET4US	false
172.29.49.222	unknown	Reserved		7018	ATT-INTERNET4US	false
85.22.167.142	unknown	Germany		15763	ASDOKOMDE	false
112.243.121.18	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
31.195.173.100	unknown	Italy		3269	ASN-IBSNAZIT	false
95.19.24.254	unknown	Spain		12479	UNI2-ASES	false
62.86.66.122	unknown	Italy		3269	ASN-IBSNAZIT	false
37.35.209.230	unknown	Spain		12479	UNI2-ASES	false
95.231.17.245	unknown	Italy		3269	ASN-IBSNAZIT	false
85.211.15.176	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
172.12.143.82	unknown	United States		7018	ATT-INTERNET4US	false
157.251.170.211	unknown	United States		32934	FACEBOOKUS	false
109.48.129.122	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
62.242.237.55	unknown	Denmark		3292	TDCTDCASDK	false
98.71.213.216	unknown	United States		7018	ATT-INTERNET4US	false
42.94.84.8	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
31.100.145.23	unknown	United Kingdom		12576	EELtdGB	false
172.232.64.132	unknown	United States		20940	AKAMAI-ASN1EU	false
79.56.176.165	unknown	Italy		3269	ASN-IBSNAZIT	false
94.153.184.213	unknown	Ukraine		15895	KSNET-ASUA	false
95.117.176.77	unknown	Germany		6805	TDDE-ASN1DE	false
94.78.81.202	unknown	Turkey		44558	NETONLINETR	false
184.205.26.70	unknown	United States		10507	SPCSUS	false
94.122.78.64	unknown	Turkey		12978	DOGAN-ONLINETR	false
98.25.94.209	unknown	United States		11426	TWC-11426-CAROLINASUS	false
85.95.179.143	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
94.72.179.78	unknown	Bulgaria		42735	MAXTELECOM-ASBG	false
5.75.234.238	unknown	Germany		24940	HETZNER-ASDE	false
2.243.0.76	unknown	Germany		6805	TDDE-ASN1DE	false
98.155.194.67	unknown	United States		20001	TWC-20001-PACWESTUS	false
95.50.145.214	unknown	Poland		5617	TPNETPL	false
172.75.35.52	unknown	United States		11426	TWC-11426-CAROLINASUS	false
95.76.74.122	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
94.137.178.61	unknown	Georgia		16010	MAGTICOMASCaucasus-OnlineGE	false
94.35.200.82	unknown	Italy		8612	TISCALI-IT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.38.6.178	unknown	France		5410	BOUYGTEL-ISPFR	false
172.132.181.16	unknown	United States		7018	ATT-INTERNET4US	false
197.141.89.106	unknown	Algeria		36891	ICOSNET-ASDZ	false
172.75.250.68	unknown	United States		11426	TWC-11426-CAROLINASUS	false
197.210.99.198	unknown	Nigeria		29465	VCG-ASNG	false
184.11.39.229	unknown	United States		5650	FRONTIER-FRTRUS	false
98.46.226.92	unknown	United States		7922	COMCAST-7922US	false
42.8.182.129	unknown	Korea Republic of		4249	LILLY-ASUS	false
95.52.196.251	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
95.212.143.38	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
2.184.242.157	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
98.142.17.21	unknown	United States		22402	NEXTCO-ASUS	false
184.161.229.5	unknown	Canada		5769	VIDEOTRONCA	false
172.65.108.232	unknown	United States		13335	CLOUDFLARENETUS	false
62.184.255.131	unknown	European Union		34456	RIALCOM-ASRU	false
172.125.131.77	unknown	United States		7018	ATT-INTERNET4US	false
85.48.206.171	unknown	Spain		12479	UNI2-ASES	false
184.223.3.10	unknown	United States		10507	SPCSUS	false
41.240.121.98	unknown	Sudan		36998	SDN-MOBITELSD	false
172.197.166.158	unknown	Australia		18747	IFX18747US	false
85.173.96.247	unknown	Russian Federation		43132	KBT-ASBranchformerKabbalktelecomRU	false
62.215.147.66	unknown	Kuwait		21050	FAST-TELCOKW	false
31.191.242.132	unknown	Italy		24608	WINDTRE-ASIT	false
184.239.67.225	unknown	United States		10507	SPCSUS	false
98.69.167.71	unknown	United States		7018	ATT-INTERNET4US	false
197.70.138.200	unknown	South Africa		16637	MTNNS-ASZA	false
172.75.35.39	unknown	United States		11426	TWC-11426-CAROLINASUS	false
85.90.55.74	unknown	United Kingdom		39116	TELEHOUSEGB	false
98.142.17.14	unknown	United States		22402	NEXTCO-ASUS	false
41.186.122.57	unknown	Rwanda		36890	MTNRW-ASNRW	false
95.253.111.25	unknown	Italy		3269	ASN-IBSNAZIT	false
184.89.200.166	unknown	United States		33363	BHN-33363US	false
184.14.58.56	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
95.89.255.122	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
95.110.130.123	unknown	Italy		31034	ARUBA-ASNIT	false
112.101.3.131	unknown	China		17897	CHINATELECOM-HLJ-AS-APasnforHeilongjiangProvincialNeto	false
98.167.233.126	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
94.178.33.141	unknown	Ukraine		6849	UKRTELNETUA	false

Runtime Messages

Command:	/tmp/HgTC70XRum
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	kebabware installed
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
94.70.69.92	piqPVqHVB8	Get hash	malicious	Browse	
95.6.137.29	fEbFnRr00C	Get hash	malicious	Browse	
172.150.130.143	Tsunami.arm7	Get hash	malicious	Browse	
85.230.40.164	8r3HRghvXX	Get hash	malicious	Browse	
31.136.150.35	d8dgn3wGJL	Get hash	malicious	Browse	
172.227.134.124	Tsunami.x86	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	Ceji2MdFHD	Get hash	malicious	Browse	• 42.236.166.2
	Tsunami.x86	Get hash	malicious	Browse	• 157.2.30.58
	Tsunami.arm	Get hash	malicious	Browse	• 112.249.44.124
	ivImhRZqGa	Get hash	malicious	Browse	• 27.14.154.99
	KXAJjgoH22	Get hash	malicious	Browse	• 153.65.71.169
	Z7QqCH0bak	Get hash	malicious	Browse	• 27.0.151.69
	zouBbQwUTb	Get hash	malicious	Browse	• 221.208.165.85
	0r73kbzSGC	Get hash	malicious	Browse	• 120.14.50.209
	PpZvxl4DJg	Get hash	malicious	Browse	• 60.24.162.254
	AoebJMZz3p.exe	Get hash	malicious	Browse	• 218.12.76.163
	arm7	Get hash	malicious	Browse	• 124.128.204.83
	x86_64	Get hash	malicious	Browse	• 123.148.206.41
	Dy4UCGJRnG	Get hash	malicious	Browse	• 112.245.21 2.135
	nUDLlJvoP4	Get hash	malicious	Browse	• 119.117.83.209
	9QPGr9LMaq	Get hash	malicious	Browse	• 171.124.229.97
	dqnskKAmQq	Get hash	malicious	Browse	• 112.245.183.97
	A0Pvsxsjf7	Get hash	malicious	Browse	• 27.200.159.23
	5odXR1ZmTd	Get hash	malicious	Browse	• 27.200.159.13
	x86	Get hash	malicious	Browse	• 27.212.245.135
	2pPPNW1XSo	Get hash	malicious	Browse	• 115.50.250.171
CLODO-ASRU	A0Pvsxsjf7	Get hash	malicious	Browse	• 85.143.199.237
	HF0udkDj2N	Get hash	malicious	Browse	• 85.143.199.211
	0OxK4NR2wM	Get hash	malicious	Browse	• 85.143.199.231
	x.arm7	Get hash	malicious	Browse	• 85.143.199.200
	dLOVD1avSg	Get hash	malicious	Browse	• 85.143.199.200
	21BHS9gNtk	Get hash	malicious	Browse	• 85.143.199.226
	aUXe29TOLB	Get hash	malicious	Browse	• 85.143.199.235
	UnHAnaAW.arm7	Get hash	malicious	Browse	• 85.143.199.209
	UnHAnaAW.x86	Get hash	malicious	Browse	• 85.143.199.239
	R0zLx1X0D0	Get hash	malicious	Browse	• 85.143.199.238
	peach.arm	Get hash	malicious	Browse	• 62.76.187.121
	s2w2tmw8l0	Get hash	malicious	Browse	• 85.143.199.245
	x86	Get hash	malicious	Browse	• 85.143.199.219
	1GDjPopt8R	Get hash	malicious	Browse	• 62.76.187.111
	81NEPOIyrA	Get hash	malicious	Browse	• 85.143.199.231
	lBuWpqnzMD	Get hash	malicious	Browse	• 85.143.199.240
	popsmoke.mpsl	Get hash	malicious	Browse	• 85.143.199.246
	1.sh	Get hash	malicious	Browse	• 62.76.188.184
	1105_748543.doc	Get hash	malicious	Browse	• 62.76.40.132
	fvwOOeZ5IE.exe	Get hash	malicious	Browse	• 62.76.40.132

JA3 Fingerprints

No context

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.

/memfd:30-systemd-environment-d-generator (deleted)	
Process:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
File Type:	ASCII text
Category:	dropped
Size (bytes):	200
Entropy (8bit):	4.621490641385995
Encrypted:	false
SSDEEP:	3:+2snsY7+4VMPQnMLmPQ9JEcn8YLw6mNErZwb906izhs32Y0f/KiDXK/vi++BLiVv:Ess+4m4Mixc8Y06me6osMjDXj++yvn
MD5:	5EF9649F7C218F464C253BDC1549C046
SHA1:	07C3B1103F09E5FB0B4701E75E326D55D4FC570B
SHA-256:	B4480A805024063034CB27A4A70BCA625C46C98963A39FE18F9BE2C499F1DA40
SHA-512:	DF620669CD92538F00FEB397BA8BB0C0DC9E242BA2A3F25561DE20AE59B73AC54A15DBFBD4C43F8006FA09D0A07D9EC5DD5D395AD4746E022A17E78274DEB3B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	QT_ACCESSIBILITY=1.PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin.XDG_DATA_DIRS=/usr/local/share/:/usr/share/:/var/lib/snapd/desktop.

/memfd:user-environment-generators (deleted)	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	212
Entropy (8bit):	4.657790370557215
Encrypted:	false
SSDEEP:	6:ulsT4m4Mixc8Y06me6kLT0QsMjDXj++yvn:XT5ikXT05OLj+Hvn
MD5:	769AC00395ABDA061DA4777C87620B21

/memfd:user-environment-generators (deleted)	
SHA1:	AC12A8E0EB413395C64577FA7E514626B8F8F548
SHA-256:	75867CD2977A9A9AAB70E70CFEE3C20151F31C9B3CBDA4A81C06627C291D2C82
SHA-512:	67C2B17CDD15B7F69BE2DF4F3136E3F393C1C6F990755DFEEC1B0B4E1081A15132A8D77A1624CAD1F6255591AE54CB9135F1B94FE31D5876E2A17B215CDB78F3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	env=QT_ACCESSIBILITY=1.env=PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin.env=XDG_DATA_DIRS=/usr/local/share/:/usr/share/:/var/lib/snapd/desktop.

/proc/5277/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:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/proc/5779/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0

/proc/5847/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:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Preview:	-1000.

/proc/6672/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped

/proc/6672/oom_score_adj	
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
Preview:	 -1000.

/proc/6681/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/7082/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
Preview:	 -1000.

/proc/7485/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
Preview:	 -1000.

/proc/7503/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)

/proc/7503/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

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:id6:ic
MD5:	262A9A549E40FF4C89D183BF97773B8C
SHA1:	3EBC8000AEAB999EC75856FD6FE9912B2E2D41C3
SHA-256:	1B81AD4FB5F8B92B63539150FB17F478BFFC82D2D25F064E7CD534333B572B79
SHA-512:	46F97981E1D583AE1E278CE24EE2F8466B1B721F4A34B93C6A8295F71D699B12B89973A894515670A67D1435D8ABA581E1ABD0ACB5DAD59F30D39B7D6D6FE09 B
Malicious:	false
Preview:	 7485.

/run/systemd/inhibit/.#10ZPzBxH	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.1334532270294
Encrypted:	false
SSDEEP:	6:SbFuFyL8NEL1QXccIRI/cIIG/cI/0tmWvyPXaLX6zpp7Rl:qgFqXQXTI1lltIQvEy0Rl
MD5:	AF66846AF74C40610BAFB25EE938E4A4
SHA1:	FE0B6DDD55722B8EF394C736B3868CFF6744AADB
SHA-256:	BD8502E132D917AEBA0DBEC8BC8A7577225E2292D5DFCA93E7BF8E9676749D7E
SHA-512:	382125456440D04D4C16AEAF60066659FEFC4F14AF76A215901DD2AC13E1C24FB37F0C13BA9BD5CE7D32633544658FB855834084CC69576FEEEBF96BBB7D9ED D
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=handle-power-key:handle-suspend-key:handle-hibernate-key:handle-lid-switch.MODE=block.UID=1000.PID=2123.WHO =xfce4-power-manager.WHY=xfce4-power-manager handles these events.FIFO=/run/systemd/inhibit/10.ref.

/run/systemd/inhibit/.#12nWurb	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#16hWgQX	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1EGlZZP	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1RlzkGY	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1Re4DeT	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1S68Cxb	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1b8gRAE	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1nh7Pml	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1olC5W2	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run /systemd/inhibit/1.ref.

/run/systemd/inhibit/.#1zJWT43	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.963022897344031
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifVmDkBoDWicRF2Tg+tX8/Sf9n:SbFuFyL8OAApfADjDJcjKR9n
MD5:	740A3D9E5BDC608745C17F00098F3B54
SHA1:	7560EFF166E352223840BEC1F56A81E2E750EAA4
SHA-256:	2E4D26DB81D842D45D86636831C89D683C5E76402507208EE127B8BCFDF761A5
SHA-512:	1B4A026AF214E8797A267CB75D1201E8B4A2C56C95C9A02EB928F77CF2ADB9FB196107163436B30801AE0AE15D67934224F58AB590F94E12ED962389C38AD675
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=847.WHO=ModemManager.WHY=ModemManager needs to reset devices.FIFO=/run/systemd/inhibit/1.ref.

/run/systemd/inhibit/.#3tywmCE	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.981193950793451
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWNQK4wq29ifx+q+zgCtkBFqG8QCfA/dcvWZ47tX8/SfWADv:SbFuFyL8KQKeLfUq6gckMQ22dKWZAlRT
MD5:	A1C4614191983B812562258CC03B7BB1
SHA1:	1B6B9CE5685DDE148191EB555E97315711649F50
SHA-256:	7AFBD3A498991585285E7B73720083EAFC602DD1310D179FF8C3772F98E21134
SHA-512:	A16EF07B928AFE1779BA2E154641039206ECA3F219DE48163D31BFC91FD4313DADAF771EE4269E3CC03B89C81C759A28310BD24D701E5B3DBF8036C226B4B32
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=shutdown.MODE=delay.UID=0.PID=884.WHO=Unattended Upgrades Shutdown.WHY=Stop ongoing upgrades or perform upgrades before shutdown.FIFO=/run/systemd/inhibit/3.ref.

/run/systemd/inhibit/.#430oBeH	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.109910338925392
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifSU1IppTMXSHK72X8/SflY:SbFuFyL8OAApfZApLHK7wRS
MD5:	E374D3E418E44E444D586B8A667BA7B9
SHA1:	10E313EA3C86F242B0921AB80E794817F858DE3C
SHA-256:	E3C381103F615FE4A0F85F9F07DBD40A4E8DB91EAA187D48472C7EEC6772C23C
SHA-512:	42AD26F8C651EF390A526392C492526AA81919D09085D7DB9A6DE067AADEE06AA8E908638667AFAE1A79F2C632E430868E9D87D36BF45DE0E708BFE83993E99
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=1599.WHO=UPower.WHY=Pause device polling.FIFO=/run/systemd/inhibit/4.ref.

/run/systemd/inhibit/.#471I1xY	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.109910338925392
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifSU1IppTMXSHK72X8/SflY:SbFuFyL8OAApfZApLHK7wRS
MD5:	E374D3E418E44E444D586B8A667BA7B9
SHA1:	10E313EA3C86F242B0921AB80E794817F858DE3C
SHA-256:	E3C381103F615FE4A0F85F9F07DBD40A4E8DB91EAA187D48472C7EEC6772C23C
SHA-512:	42AD26F8C651EF390A526392C492526AA81919D09085D7DB9A6DE067AADEE06AA8E908638667AFAE1A79F2C632E430868E9D87D36BF45DE0E708BFE83993E99
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=1599.WHO=UPower.WHY=Pause device polling.FIFO=/run/systemd/inhibit/4.ref.

/run/systemd/inhibit/.#4QUeelS	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.109910338925392
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifSU1IppTMXSHK72X8/SflY:SbFuFyL8OAApfZApLHK7wRS
MD5:	E374D3E418E44E444D586B8A667BA7B9
SHA1:	10E313EA3C86F242B0921AB80E794817F858DE3C
SHA-256:	E3C381103F615FE4A0F85F9F07DBD40A4E8DB91EAA187D48472C7EEC6772C23C
SHA-512:	42AD26F8C651EF390A526392C492526AA81919D09085D7DB9A6DE067AADEE06AA8E908638667AFAE1A79F2C632E430868E9D87D36BF45DE0E708BFE83993E99
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=1599.WHO=UPower.WHY=Pause device polling.FIFO=/run/systemd/inhibit/4.ref.

/run/systemd/inhibit/.#4WFfqZ2	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.109910338925392
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifSU1IppTMXSHK72X8/SflY:SbFuFyL8OAApfZApLHK7wRS
MD5:	E374D3E418E44E444D586B8A667BA7B9
SHA1:	10E313EA3C86F242B0921AB80E794817F858DE3C
SHA-256:	E3C381103F615FE4A0F85F9F07DBD40A4E8DB91EAA187D48472C7EEC6772C23C
SHA-512:	42AD26F8C651EF390A526392C492526AA81919D09085D7DB9A6DE067AADEE06AA8E908638667AFAE1A79F2C632E430868E9D87D36BF45DE0E708BFE83993E99
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=1599.WHO=UPower.WHY=Pause device polling.FIFO=/run/systemd/inhibit/4.ref.

/run/systemd/inhibit/.#4qAQ4da	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.109910338925392
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifSU1IppTMXSHK72X8/SflY:SbFuFyL8OAApfZApLHK7wRS
MD5:	E374D3E418E44E444D586B8A667BA7B9
SHA1:	10E313EA3C86F242B0921AB80E794817F858DE3C
SHA-256:	E3C381103F615FE4A0F85F9F07DBD40A4E8DB91EAA187D48472C7EEC6772C23C
SHA-512:	42AD26F8C651EF390A526392C492526AA81919D09085D7DB9A6DE067AADEE06AA8E908638667AFAE1A79F2C632E430868E9D87D36BF45DE0E708BFE83993E99
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=1599.WHO=UPower.WHY=Pause device polling.FIFO=/run/systemd/inhibit/4.ref.

/run/systemd/inhibit/.#5nR6tNF	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.229502665506919
Encrypted:	false
SSDEEP:	6:SbFuFyL8NEL1QXccIRI/cIlGjdC+5rqKLXv0R5:qgFqXQXTI1Il0qKjcR5
MD5:	65D49247D84F1F59B04E2D62ACBF37DF
SHA1:	0769B6966C4C44D013DCD3ADD8297BBD3712BF05
SHA-256:	3F5664EB8E0E6A758DE79C7731E3CEC1C794732476C842DD057932D67D3812D5
SHA-512:	E1B4834B171FF12BD80BCD5261E3EEAABD61766CC6A3BFFD8195A0C87345601207257B0B1CF03388B494523AE1FA6BDFFB82EFE25E885A3E8BB5824A04F8702D
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=handle-power-key:handle-suspend-key:handle-hibernate-key.MODE=block.UID=127.PID=1648.WHO=gdm.WHY=GNOME handling keypresses.FIFO=/run/systemd/inhibit/5.ref.

/run/systemd/inhibit/.#64bqCRG	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.1669277917692895
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9c+5ViXoqKZLXviX8/SfI:SbFuFyL8OAAx+5rqKLXv0RI
MD5:	95B4BEB9E23C631D44BA23687078DEAB
SHA1:	E8858CA80C412C790D383760A0CD031213EF30A2
SHA-256:	3A02E7AD5FD819002373D84A62069BE9522E9F994400633DD477B4789C0616C0
SHA-512:	BA3AB070840AD50CA3A630455B351ECE9CB2D89E6C32FA0C43BA869AF571AE8D63AE83AF95742A145DE89B095D1BC64BC0682995FDC56FE95A3BC3439DF2F732
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=127.PID=1648.WHO=gdm.WHY=GNOME handling keypresses.FIFO=/run/systemd/inhibit/6.ref.

/run/systemd/inhibit/.#7ftr1zH	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.138883971711133
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9c+5lyiiXuIpv5RX8/Sffn:SbFuFyL8OAAx+5lNlpLRfn
MD5:	9921B6FC71927A90C0CEB5BCA4748393
SHA1:	0376F45428203428F5E9C156A981044E2D66333C
SHA-256:	EB6B7209CD410B6CC4E42E26224BEC45C9935357F5574FB2B8DCBDFB955BAFA6
SHA-512:	279E8A47E3A3269CF04ABEA70CC4E92FCEBE56F1A9D1539C1D6BF9085F876A2C740C940DF5018E396C6CA463A71BE0B71DB90E0D699B4398E38FA72B55BE56C
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=127.PID=1668.WHO=gdm.WHY=GNOME needs to lock the screen.FIFO=/run/systemd/inhibit/7.ref.

/run/systemd/inhibit/.#81EP26G	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	164
Entropy (8bit):	5.11427950700706
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9hFfy3GXA6wTgvWvVZX8/Sf+Dvn:SbFuFyL8OAAKfy3GXxVWNpR+z
MD5:	A2809D1B173C22623712906FBB235B53
SHA1:	8D1481F5BA5D1F7FC25FF2CD90B553A9D92DF84B
SHA-256:	DF533496FEFF7669BA95EFA1AA09BCBEF7440FCA20042DA62231C1E6D5F2365D
SHA-512:	8FBC45A480B6FB4FD3CDCD2D94209B551F3C0B7C8F94AC57F6B00FA9D156D3A7D6A586F213F613A3726EB227348EEC42B7D209274AB3D8111C1C4F7AD073706
Malicious:	false
Preview:	# This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=1000.PID=2028.WHO=xfce4-screensaver.WHY=Locking screen before sleep.FIFO=/run/systemd/inhibit/8.ref.

/run/systemd/resolve/.#resolv.confBal8An	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.60400988248083
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAS5wtRZ6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgvArHW:qmmIz07IuKD24CUB3Og2Tca
MD5:	DAC2BDC6F091CE9ED180809307F777AE
SHA1:	3A8F59FD68419F9C574C3A9D04E3AA76D6343EC1
SHA-256:	4EF31D415ECE44921919EFA070C04F3F43945336D75D4C1E7354637BCD20DCDD
SHA-512:	F23E4320950F84461552D438F264B17DEB2747061FD13F8A435DAF810E53CBCDAC77122A2B7382DE484931D469EDEF4A52C19EEDB01CEFD5A63D4AB7B6DB260
Malicious:	false

/run/systemd/resolve/.#resolv.confBal8An	
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients directly to.# all known uplink DNS servers. This file lists all configured search domains..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 1.1.1.1.nameserver 8.8.8.8.

/run/systemd/resolve/.#resolv.confO30xD5	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.60400988248083
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAS5wtRZ6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgvArHW:qmmIz07IuKD24CUB3Og2Tca
MD5:	DAC2BDC6F091CE9ED180809307F777AE
SHA1:	3A8F59FD68419F9C574C3A9D04E3AA76D6343EC1
SHA-256:	4EF31D415ECE44921919EFA070C04F3F43945336D75D4C1E7354637BCD20DCDD
SHA-512:	F23E4320950F84461552D438F264B17DEB2747061FD13F8A435DAF810E53CBCDAC77122A2B7382DE484931D469EDEF4A52C19EEDB01CEFD5A63D4AB7B6DB26 0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients directly to.# all known uplink DNS servers. This file lists all configured search domains..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 1.1.1.1.nameserver 8.8.8.8.

/run/systemd/resolve/.#resolv.confSX8WU7	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.60400988248083
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAS5wtRZ6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgvArHW:qmmIz07IuKD24CUB3Og2Tca
MD5:	DAC2BDC6F091CE9ED180809307F777AE
SHA1:	3A8F59FD68419F9C574C3A9D04E3AA76D6343EC1
SHA-256:	4EF31D415ECE44921919EFA070C04F3F43945336D75D4C1E7354637BCD20DCDD
SHA-512:	F23E4320950F84461552D438F264B17DEB2747061FD13F8A435DAF810E53CBCDAC77122A2B7382DE484931D469EDEF4A52C19EEDB01CEFD5A63D4AB7B6DB26 0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients directly to.# all known uplink DNS servers. This file lists all configured search domains..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 1.1.1.1.nameserver 8.8.8.8.

/run/systemd/resolve/.#resolv.confuBqyz6	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.60400988248083
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAS5wtRZ6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgvArHW:qmmIz07IuKD24CUB3Og2Tca
MD5:	DAC2BDC6F091CE9ED180809307F777AE
SHA1:	3A8F59FD68419F9C574C3A9D04E3AA76D6343EC1
SHA-256:	4EF31D415ECE44921919EFA070C04F3F43945336D75D4C1E7354637BCD20DCDD
SHA-512:	F23E4320950F84461552D438F264B17DEB2747061FD13F8A435DAF810E53CBCDAC77122A2B7382DE484931D469EDEF4A52C19EEDB01CEFD5A63D4AB7B6DB26 0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients directly to.# all known uplink DNS servers. This file lists all configured search domains..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 1.1.1.1.nameserver 8.8.8.8.

/run/systemd/resolve/.#resolv.confxhPTt5	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped

/run/systemd/resolve/.#resolv.confxhPTt5	
Size (bytes):	603
Entropy (8bit):	4.60400988248083
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAS5wtRZ6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgvArHW:qmmIz07IuKD24CUB3Og2Tca
MD5:	DAC2BDC6F091CE9ED180809307F777AE
SHA1:	3A8F59FD68419F9C574C3A9D04E3AA76D6343EC1
SHA-256:	4EF31D415ECE44921919EFA070C04F3F43945336D75D4C1E7354637BCD20DCDD
SHA-512:	F23E4320950F84461552D438F264B17DEB2747061FD13F8A435DAF810E53CBCDAC77122A2B7382DE484931D469EDEF4A52C19EEDB01CEFD5A63D4AB7B6DB26 0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients directly to.# all known uplink DNS ser vers. This file lists all configured search domains..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 1.1.1.1.nameserver 8.8.8.8.

/run/systemd/resolve/.#stub-resolv.conf66MvJ5	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	717
Entropy (8bit):	4.618141658133841
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAYEcWcXxRdxwlvj+ScH6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgF:qmmIREPcXxnxwIRcHIuKD24CUB3Og2TX
MD5:	FBFDE622AE28A4DCFBF73A397A10C6AE
SHA1:	E6B5915B590FC5A4FB484D2E456E76466DB7BD17
SHA-256:	DBEFE28051828B529E2299A83A76F268A8CF9FE686B1FA09DEC61F7AB1222658
SHA-512:	C966F0F8483378A55654A40B2ED05F1C4057D11BBB8C83D4BAA9921460C8028CF71FCA2E08DAFAB2C7C421FCDBDD7ABD78BF951DC2D9416547A5579E925CC F0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients to the.# internal DNS stub resolver of systemd-resolved. This file lists all.# configured search domains..#.# Run "resolvectl status" to see details about the uplink DNS servers.# currently in use..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 127.0.0 .53.options edns0 trust-ad.

/run/systemd/resolve/.#stub-resolv.confl4xv33	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	717
Entropy (8bit):	4.618141658133841
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAYEcWcXxRdxwlvj+ScH6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgF:qmmIREPcXxnxwIRcHIuKD24CUB3Og2TX
MD5:	FBFDE622AE28A4DCFBF73A397A10C6AE
SHA1:	E6B5915B590FC5A4FB484D2E456E76466DB7BD17
SHA-256:	DBEFE28051828B529E2299A83A76F268A8CF9FE686B1FA09DEC61F7AB1222658
SHA-512:	C966F0F8483378A55654A40B2ED05F1C4057D11BBB8C83D4BAA9921460C8028CF71FCA2E08DAFAB2C7C421FCDBDD7ABD78BF951DC2D9416547A5579E925CC F0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients to the.# internal DNS stub resolver of systemd-resolved. This file lists all.# configured search domains..#.# Run "resolvectl status" to see details about the uplink DNS servers.# currently in use..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 127.0.0 .53.options edns0 trust-ad.

/run/systemd/resolve/.#stub-resolv.confPyn415	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	717
Entropy (8bit):	4.618141658133841
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAYEcWcXxRdxwlvj+ScH6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgF:qmmIREPcXxnxwIRcHIuKD24CUB3Og2TX
MD5:	FBFDE622AE28A4DCFBF73A397A10C6AE
SHA1:	E6B5915B590FC5A4FB484D2E456E76466DB7BD17
SHA-256:	DBEFE28051828B529E2299A83A76F268A8CF9FE686B1FA09DEC61F7AB1222658

/run/systemd/resolve/.#stub-resolv.confPyn415	
SHA-512:	C966F0F8483378A55654A40B2ED05F1C4057D11BBB8C83D4BAA9921460C8028CF71FCA2E08DAFAB2C7C421FCDBDD7ABD78BF951DC2D9416547A5579E925CCF0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients to the.# internal DNS stub resolver of systemd-resolved. This file lists all.# configured search domains..#.# Run "resolvectl status" to see details about the uplink DNS servers.# currently in use..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 127.0.0.53.options edns0 trust-ad.

/run/systemd/resolve/.#stub-resolv.confsxiLlo	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	717
Entropy (8bit):	4.618141658133841
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAYEcWcXxRdxwlvj+ScH6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgF:qmmIREPcXxnxwIRcHIuKD24CUB3Og2TX
MD5:	FBFDE622AE28A4DCFBF73A397A10C6AE
SHA1:	E6B5915B590FC5A4FB484D2E456E76466DB7BD17
SHA-256:	DBEFE28051828B529E2299A83A76F268A8CF9FE686B1FA09DEC61F7AB1222658
SHA-512:	C966F0F8483378A55654A40B2ED05F1C4057D11BBB8C83D4BAA9921460C8028CF71FCA2E08DAFAB2C7C421FCDBDD7ABD78BF951DC2D9416547A5579E925CCF0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients to the.# internal DNS stub resolver of systemd-resolved. This file lists all.# configured search domains..#.# Run "resolvectl status" to see details about the uplink DNS servers.# currently in use..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 127.0.0.53.options edns0 trust-ad.

/run/systemd/resolve/.#stub-resolv.confwDzMga	
Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	717
Entropy (8bit):	4.618141658133841
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAYEcWcXxRdxwlvj+ScH6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgF:qmmIREPcXxnxwIRcHIuKD24CUB3Og2TX
MD5:	FBFDE622AE28A4DCFBF73A397A10C6AE
SHA1:	E6B5915B590FC5A4FB484D2E456E76466DB7BD17
SHA-256:	DBEFE28051828B529E2299A83A76F268A8CF9FE686B1FA09DEC61F7AB1222658
SHA-512:	C966F0F8483378A55654A40B2ED05F1C4057D11BBB8C83D4BAA9921460C8028CF71FCA2E08DAFAB2C7C421FCDBDD7ABD78BF951DC2D9416547A5579E925CCF0
Malicious:	false
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients to the.# internal DNS stub resolver of systemd-resolved. This file lists all.# configured search domains..#.# Run "resolvectl status" to see details about the uplink DNS servers.# currently in use..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 127.0.0.53.options edns0 trust-ad.

/run/systemd/seats/.#seat0AMqo9P	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D04C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0EN6CMX	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0J28c9F	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0Nc4xK5	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.957035419463244
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+ugKQ2KwshcXSv:SbFuFyLwH47Pg20ggWunQ2rNXc
MD5:	66D114877B3B4DB3BDD8A3AD4F5E7421
SHA1:	62E0CB0F51E0E3F97BE251CB917968DFF69ED344
SHA-256:	A922628916A7DDBE2BAA33F421C82250527EA3C28E429749353A1C75C0C18860
SHA-512:	5651247FA236DCF020A3C8456E4A9A74A85C5B9B3CCE94A3CF8F85FD4D66465C9F97DF7A1822E6CA4553C02BE149F3021D58DCC0C8CB6DCF37F915BD0A15817
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.SESSIONS=c1.UIDS=127.

/run/systemd/seats/.#seat0Pl5WYE	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.957035419463244
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+ugKQ2KwshcXSv:SbFuFyLwH47Pg20ggWunQ2rNXc
MD5:	66D114877B3B4DB3BDD8A3AD4F5E7421
SHA1:	62E0CB0F51E0E3F97BE251CB917968DFF69ED344
SHA-256:	A922628916A7DDBE2BAA33F421C82250527EA3C28E429749353A1C75C0C18860
SHA-512:	5651247FA236DCF020A3C8456E4A9A74A85C5B9B3CCE94A3CF8F85FD4D66465C9F97DF7A1822E6CA4553C02BE149F3021D58DCC0C8CB6DCF37F915BD0A15817
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.SESSIONS=c1.UIDS=127.

/run/systemd/seats/.#seat0Rap2Va	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/seats/.#seat0W56IiW	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.957035419463244
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+ugKQ2KwshcXSv:SbFuFyLwH47Pg20ggWunQ2rNXc
MD5:	66D114877B3B4DB3BDD8A3AD4F5E7421
SHA1:	62E0CB0F51E0E3F97BE251CB917968DFF69ED344
SHA-256:	A922628916A7DDBE2BAA33F421C82250527EA3C28E429749353A1C75C0C18860
SHA-512:	5651247FA236DCF020A3C8456E4A9A74A85C5B9B3CCE94A3CF8F85FD4D66465C9F97DF7A1822E6CA4553C02BE149F3021D58DCC0C8CB6DCF37F915BD0A15817
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.SESSIONS=c1.UIDS=127.

/run/systemd/seats/.#seat0fl6403	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/systemd/users/.#1271RfBJF	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.274997718721799
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgdNR2sKiYiesnAv/XSHxJgCCqhajT56H206qodav:SbFuFyL3BVgdL87iesnAiRJgCC5jT5iJ
MD5:	15400B293B0D101D1111001ABA4D90CE
SHA1:	492C5FB0E2018F7A8CD2ED4111A14CF2563B0D0C
SHA-256:	3E96755531C81ACB43664F3FC8960997786F0A196B4A9903C090F2B0860FB517
SHA-512:	076E113A846FB9BD0858525EC33C51163B91A2B17A240F2EA5EE6DD700A8FE751AC787804D2741968C9CEC0DC87919B3F1FB240E168D978E7FD4D8222001829
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=no.RUNTIME=/run/user/127.REALTIME=1635742357753073.MONOTONIC=455268750.LAST_SESSION_TIMESTAMP=455337740.

/run/systemd/users/.#1272Ctk1E	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4559066563533
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0IxffPWzgCC5jT5it6C:qgFq30dABibB2zgboIC
MD5:	2DC275AB64C26287BE7EF40011FDB661
SHA1:	E8C814F59C3AFF4ED183D968E8B46BB562E2B172
SHA-256:	FEBF50E921A24E9DEDE8879B250840B976E5A850AFBE03D5EB06011E2F244EB8
SHA-512:	4878861D9538C573D4A520F722B510D1BD4695FA7549B9F52220952D0C29246BBC48C2CCBF63F0EE97FA16152D0955F293363379FAC65209407B4D99FDC08FE9
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=yes.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/11863.REALTIME=1635742357753073.MONOTONIC=455268750.LAST_SESSION_TIMESTAMP=455337740.

/run/systemd/users/.#127GOTvGV	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.321113364258541
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6e/TgCEoq+8T12thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBdTgwC8thQHtPYq9M
MD5:	668BB14292207B4193FBD0165212D791
SHA1:	1B1332588FC7F4FADA83592AD55521C1E33A20AF
SHA-256:	F1DCFB249ED086DC16E57CC207CC42F91DBDF061E3765624CCF77CAC3E518352
SHA-512:	21495272AC31BE5410444B50D3F31043C5D51874DCB132912B7BB9094850B1D1BFC13C806AC7819445D975807D43C3283136DA8DED07F8E41EAD991FF1F4D203
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12612.REALTIME=1635742485780289.MONOTONIC=583295966.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127HLkUr3	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.297320259519998
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgdNR2sKiYiesnAv/XSHxJgCyHvbK4zjRAt8H206qodv5Wv:SbFuFyL3BVgdL87iesnAiRJgC9gt6zo
MD5:	03393A797384600D826862DB0186AB39
SHA1:	5AC5F81B0A8A0145425F40173BAB762D4D824E39
SHA-256:	2CC019EE2A614536F8098FD778EAFF79D6E45355170D31611352C10E9A0E9C5E
SHA-512:	681114165A57024A48AA3C263921410D02C488FB427C9BC4B7E3ABEF7A0EBBBBE69F3CD3C353D4AB485F94B0402F1ED71862714D3328FCAA3380A261772D331
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=no.RUNTIME=/run/user/127.REALTIME=1635742450029056.MONOTONIC=547544733.LAST_SESSION_TIMESTAMP=547625023.

/run/systemd/users/.#127K2GgTV	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	4.928997328913428
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgVuMI2sKiYiesnAv/XS12K2hwEY8mTQ2pJi22sQ2KkmD2pi:SbFuFyL3BVgVuR257iesnAi12thQc2p4
MD5:	065A3AD1A34A9903F536410ECA748105
SHA1:	21CD684DF60D569FA96EEEB66A0819EAC1B2B1A4
SHA-256:	E80554BF0FF4E32C61D4FA3054F8EFB27A26F1C37C91AE4EA94445C400693941
SHA-512:	DB3C42E893640BAEE9F0001BDE6E93ED40CC33198AC2B47328F577D3C71E2C2E986AAAFEF5BD8ADBC639B5C24ADF715D87034AE24B697331FF6FEC5962630064
Malicious:	false

/run/systemd/users/.#127K2GgTV	
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127TNOwe4	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.459667824699801
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0Ixff6pxJgC9gt6zo:qgFq30dABibBSgWgIzo
MD5:	C1979238FAE9AE72FB392E93CD3B3F5F
SHA1:	5498552B9AD6C4ED8D186197F31711F0C45C2F54
SHA-256:	8D0380AF9ABA05BD2FC6E318EA177910D697A9E27F7DF0CFBB1E55AB98C37BD6
SHA-512:	481D384A3D9A1515F7FA636FA2DD27F6D0EAB9F0515A13F6A54ED9D347B501EA3577293A591868307577A45E6B12C6162FA056A0608A11C3C54F82DC5E654E9C
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=yes.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12174.REALTIME=1635742450029056.MONOTONIC=547544733.LAST_SESSION_TIMESTAMP=547625023.

/run/systemd/users/.#127Ve9lrW	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.321113364258541
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6e/TgCEoq+8T12thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBdTgwC8thQHtPYq9M
MD5:	668BB14292207B4193FBD0165212D791
SHA1:	1B1332588FC7F4FADA83592AD55521C1E33A20AF
SHA-256:	F1DCFB249ED086DC16E57CC207CC42F91DBDF061E3765624CCF77CAC3E518352
SHA-512:	21495272AC31BE5410444B50D3F31043C5D51874DCB132912B7BB9094850B1D1BFC13C806AC7819445D975807D43C3283136DA8DED07F8E41EAD991FF1F4D203
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12612.REALTIME=1635742485780289.MONOTONIC=583295966.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127XwQnm6	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.29601559298621
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6dCgCGLQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBTgxthQHtPYq9M
MD5:	347DEA2A4A827F8A0CB06115C59EFC30
SHA1:	281BE0D8ED93E208487CB74698C7568AFC39DC87
SHA-256:	DB3DFBD838E325C2EC5A4E7F0EFEAA3015440CED75F966BD05BCD62196A2D43F
SHA-512:	B72C8AC2B9C37C5BBCE666FDF5CCDA400CAAE909F25F70BE60DE3FCBE677158FEA1F8C65570A22D84F887CA3890BD67CA3A0913A6C783CA6CD694B960EEAF24
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12052.REALTIME=1635742450029056.MONOTONIC=547544733.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127bb9MWH	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.4559066563533
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0IxffPWzgCC5jT5it6C:qgFq30dABibB2zgboIC
MD5:	2DC275AB64C26287BE7EF40011FDB661
SHA1:	E8C814F59C3AFF4ED183D968E8B46BB562E2B172

/run/systemd/users/.#127bb9MWH	
SHA-256:	FEBF50E921A24E9DEDE8879B250840B976E5A850AFBE03D5EB06011E2F244EB8
SHA-512:	4878861D9538C573D4A520F722B510D1BD4695FA7549B9F52220952D0C29246BBC48C2CCBF63F0EE97FA16152D0955F293363379FAC65209407B4D99FDC08FE9
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=yes.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/11863.REALTIME=1635742357753073.MONOTONIC=455268750.LAST_SESSION_TIMESTAMP=455337740.

/run/systemd/users/.#127f3wNUD	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	4.928997328913428
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs5BuSgVuMI2sKiYiesnAv/XS12K2hwEY8mTQ2pJi22sQ2KkmD2pi:SbFuFyL3BVgVuR257iesnAi12thQc2p4
MD5:	065A3AD1A34A9903F536410ECA748105
SHA1:	21CD684DF60D569FA96EEEB66A0819EAC1B2B1A4
SHA-256:	E80554BF0FF4E32C61D4FA3054F8EFB27A26F1C37C91AE4EA94445C400693941
SHA-512:	DB3C42E893640BAEE9F0001BDE6E93ED40CC33198AC2B47328F577D3C71E2C2E986AAAFEF5BD8ADBC639B5C24ADF715D87034AE24B697331FF6FEC5962630064
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127pForuI	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.292892952839982
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0IxffJUv7gCC5jhRsQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBBUv7gJRsjthQHtPYb
MD5:	8043293AF3486C82011742592EFF3886
SHA1:	D49CF9B759B33613AC08482ECE02C9A9D0C0A343
SHA-256:	01FD0181DF5F79B664859D41B864BB54A619E00FC19EF598BA7174D62F894047
SHA-512:	DEC3CF00DCE2A4ADE58970F1C8493637A5CC848A6D4684093714B897D1E44F3971550FD8622637FC0A1F3B5EFC019CFDB6455C4B1915588B277B531AF904040
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/11801.REALTIME=1635742357753073.MONOTONIC=455268750.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127rB6GJ3	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.459667824699801
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgdL87ynAir/0Ixff6pxJgC9gt6zo:qgFq30dABibBSgWgIzo
MD5:	C1979238FAE9AE72FB392E93CD3B3F5F
SHA1:	5498552B9AD6C4ED8D186197F31711F0C45C2F54
SHA-256:	8D0380AF9ABA05BD2FC6E318EA177910D697A9E27F7DF0CFBB1E55AB98C37BD6
SHA-512:	481D384A3D9A1515F7FA636FA2DD27F6D0EAB9F0515A13F6A54ED9D347B501EA3577293A5918683075 77A45E6B12C6162FA056A0608A11C3C54F82DC5E654E9C
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=closing.STOPPING=yes.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12174.REALTIME=1635742450029056.MONOTONIC=547544733.LAST_SESSION_TIMESTAMP=547625023.

/run/systemd/users/.#127yIO7w4	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	188
Entropy (8bit):	4.928997328913428
Encrypted:	false

/run/systemd/users/.#127yIO7w4	
SSDEEP:	3:SbFVVmFyinKMs5BuSgVuMI2sKiYiesnAv/XS12K2hwEY8mTQ2pJi22sQ2KkmD2pi:SbFuFyL3BVgVuR257iesnAi12thQc2p4
MD5:	065A3AD1A34A9903F536410ECA748105
SHA1:	21CD684DF60D569FA96EEEB66A0819EAC1B2B1A4
SHA-256:	E80554BF0FF4E32C61D4FA3054F8EFB27A26F1C37C91AE4EA94445C400693941
SHA-512:	DB3C42E893640BAEE9F0001BDE6E93ED40CC33198AC2B47328F577D3C71E2C2E986AAAFEF5BD8ADBC639B5C24ADF715D87034AE24B697331FF6FEC5962630064
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127z54BS2	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.29601559298621
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0Ixff6dCgCGLQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBTgxthQHtPYq9M
MD5:	347DEA2A4A827F8A0CB06115C59EFC30
SHA1:	281BE0D8ED93E208487CB74698C7568AFC39DC87
SHA-256:	DB3DFBD838E325C2EC5A4E7F0EFEAA3015440CED75F966BD05BCD62196A2D43F
SHA-512:	B72C8AC2B9C37C5BBCE666FDF5CCDA400CAAE909F25F70BE60DE3FCBE677158FEA1F8C65570A22D84F887CA3890BD67CA3A0913A6C783CA6CD694B960EEAF24
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/12052.REALTIME=1635742450029056.MONOTONIC=547544733.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/systemd/users/.#127ze3RqF	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.292892952839982
Encrypted:	false
SSDEEP:	6:SbFuFyL3BVgVuR257iesnAir/0IxffJUv7gCC5jhRsQ2thQc2pb02/g2p9rwB:qgFq30VuR8L/ibBBUv7gJRsjthQHtPYb
MD5:	8043293AF3486C82011742592EFF3886
SHA1:	D49CF9B759B33613AC08482ECE02C9A9D0C0A343
SHA-256:	01FD0181DF5F79B664859D41B864BB54A619E00FC19EF598BA7174D62F894047
SHA-512:	DEC3CF00DCE2A4ADE58970F1C8493637A5CC848A6D4684093714B897D1E44F3971550FD8622637FC0A1F3B5EFC019CFDB6455C4B1915588B277B531AF904040
Malicious:	false
Preview:	# This is private data. Do not parse..NAME=gdm.STATE=opening.STOPPING=no.RUNTIME=/run/user/127.SERVICE_JOB=/org/freedesktop/systemd1/job/11801.REALTIME=1635742357753073.MONOTONIC=455268750.SESSIONS=c1.SEATS=seat0.ACTIVE_SESSIONS=.ONLINE_SESSIONS=c1.ACTIVE_SEATS=.ONLINE_SEATS=seat0.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:HUQv:pv
MD5:	BA306AF1F3A34A69E54EACA3567DE5B7
SHA1:	4C4BF2DE981EC34D725B5270DB21111944928956
SHA-256:	F612282DB9C690F4B554215C97926895D8901C5C3BC94635731F2444DA20B8E9
SHA-512:	C840F4232423C493F6B58B7790C60660AE737E8921F327486DE55B6135C991337FBA70862B9691DF962CB90639949EADF2B88343FCC1CD544A79439DAAE153B7
Malicious:	false
Preview:	5715.

/run/user/127/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped

/run/user/127/pulse/pid	
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:gn:g
MD5:	10D9B26536B363CA179AA419C1C6DFA2
SHA1:	13DFA1C8A9315D629538238A894E7961001A6D52
SHA-256:	793709F8348FDD7B29373BA0D12EF2AA22E275D68582AD99646F2E4A7A64A84E
SHA-512:	608EFC0371EC02ADA18095D02AE21FE62E0CEB1790CE0973C74D21F892002DDA4BD243D103E8FCC64220B584B01BD66AEB524BACFEAEDF6CA2B79542B0E23E91
Malicious:	false
Preview:	6252.

/run/utmp	
Process:	/sbin/agetty
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	0.6775035134351415
Encrypted:	false
SSDEEP:	3:y0sXlXEWtl/DdEPlt:yV+ylZEd
MD5:	6D8C6B9149D531E5C62F920AAD8877A0
SHA1:	CC8B418831FC8A16265DDE0A05BA06EC5177B2A0
SHA-256:	746EC1BBD28F5E3051A1D7595456798685ED355A62EAFDF50C62AC5EDFF06DA4
SHA-512:	DF2D21B795E6CA6091F562CBCFA03D027825E3D9EF623D57FD1533160C2B938A8B97ED58356C00DDF710F23721BBBD25264D8ADA878D881042CFD310B28E6AB
Malicious:	false
Preview:	.....tty2.tty2.....tty2LOGIN.....s.a.%.....

/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/dbus.socket/cgroup.procs	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:ido:i2
MD5:	E84359125237560CABCCAA3E1D3680A6
SHA1:	922B233B9A1155EA580561B7005C194A5C2E09C5
SHA-256:	4990E43F5DA018F030E47E9E71B15DC30692AA33508451D4DEA7EAF772FA748A
SHA-512:	14752D25418B6CCFFE8A91E69C28679BFAE5F75793D6C03D819038FA01A901DFA17AA391D2B65296CF441761F867F3B52CDA009077A040D8A3734B23610FFCF1
Malicious:	false
Preview:	7483.

/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/init.scope/cgroup.procs	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.2464393446710154
Encrypted:	false
SSDEEP:	3:mdtS3en:mPn
MD5:	7D3DA9CA37AD47E8EA62E6826D293928
SHA1:	EB30016DC2997F5BBBC2E4AB22F56C21F2A85855
SHA-256:	7EB62264C547815BAE35AFA090BD73BD329FC7078E7BCFEA5FE93583BFF9E1EF
SHA-512:	B9DDF853EB7DA96A0DBDE9CD0C99B46E7C8AB4BA8314C0776A3366FF42B77C4C1FB1AABCA3FA366D0E5B0103AC02F090169F86139F4F90991A40115BDFD13FDD
Malicious:	false
Preview:	7088.7089.

/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	
Process:	/lib/systemd/systemd
File Type:	ASCII text

/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:idj:iJ
MD5:	5C1E833B957542ADD864D14F5C624264
SHA1:	E2508B077DFFDB4CD99EB77DF4854149FFD47697
SHA-256:	F5ED259D50D99D027D3B7C1B1A552AD4F6C820B0FC46D04C9BA5ED46ED886824
SHA-512:	E34B82E756163F7B78AA5AC8B7C65022BBED44D2976884DFD7811FCE8CB67E23D195435A0D9FB21EF4AE304411252221DD61D463E120316115AABB2C6D7B1FF
Malicious:	false
Preview:	7486.

/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/dbus.socket/cgroup.procs	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:ido:i2
MD5:	E84359125237560CABCCAA3E1D3680A6
SHA1:	922B233B9A1155EA580561B7005C194A5C2E09C5
SHA-256:	4990E43F5DA018F030E47E9E71B15DC30692AA33508451D4DEA7EAF772FA748A
SHA-512:	14752D25418B6CCFFE8A91E69C28679BFAE5F75793D6C03D819038FA01A901DFA17AA391D2B65296CF441761F867F3B52CDA009077A040D8A3734B23610FFCF1
Malicious:	false
Preview:	7483.

/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/init.scope/cgroup.procs	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.2464393446710154
Encrypted:	false
SSDEEP:	3:mdtS3en:mPn
MD5:	7D3DA9CA37AD47E8EA62E6826D293928
SHA1:	EB30016DC2997F5BBBC2E4AB22F56C21F2A85855
SHA-256:	7EB62264C547815BAE35AFA090BD73BD329FC7078E7BCFEA5FE93583BFF9E1EF
SHA-512:	B9DDF853EB7DA96A0DBDE9CD0C99B46E7C8AB4BA8314C0776A3366FF42B77C4C1FB1AABCA3FA366D0E5B0103AC02F090169F86139F4F90991A40115BDFD13F DD
Malicious:	false
Preview:	7088.7089.

/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	
Process:	/lib/systemd/systemd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:idj:iJ
MD5:	5C1E833B957542ADD864D14F5C624264
SHA1:	E2508B077DFFDB4CD99EB77DF4854149FFD47697
SHA-256:	F5ED259D50D99D027D3B7C1B1A552AD4F6C820B0FC46D04C9BA5ED46ED886824
SHA-512:	E34B82E756163F7B78AA5AC8B7C65022BBED44D2976884DFD7811FCE8CB67E23D195435A0D9FB21EF4AE304411252221DD61D463E120316115AABB2C6D7B1FF
Malicious:	false
Preview:	7486.

/tmp/server-0.xkm	
Process:	/usr/bin/xkbcomp
File Type:	Compiled XKB Keymap: lsb, version 15
Category:	dropped

/tmp/server-0.xkm	
Size (bytes):	12040
Entropy (8bit):	4.844996337994878
Encrypted:	false
SSDEEP:	192:QDyb2zOmnECQmwTVFfLaSLusdfVcqLkjoqdD//PJeCQ1+JdDx0s2T:QDyAxvYhFf+S62fzmp7/dMJ
MD5:	AC37A4B84E9FB5FE9E63CE9367F31371
SHA1:	E2D70CE4A01CB5F80F0C8B63EE856AE6FE8B0EFA
SHA-256:	143E089EE7EB5E9BF088C19FC59A0EA7ED061AD3AE3E3CB5BC63BDFD86833DFF
SHA-512:	3F683C4D4A3EEA88646E2BDB51BB79678B083944307811060AD0116773045F2D0245598E084310F8AC3934295E228D08B567FA6AA15FC3C9410B973AB4025664
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/lib/AccountsService/users/gdm.0OSWB1	
Process:	/usr/lib/accountsservice/accounts-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.66214589518167
Encrypted:	false
SSDEEP:	3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M
MD5:	542BA3FB41206AE43928AF1C5E61FEBC
SHA1:	F56F574DAF50D609526B36B5B54FDD59EA4D6A26
SHA-256:	730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A
SHA-512:	D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F AEA
Malicious:	false
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/AccountsService/users/gdm.IMXXB1	
Process:	/usr/lib/accountsservice/accounts-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.66214589518167
Encrypted:	false
SSDEEP:	3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M
MD5:	542BA3FB41206AE43928AF1C5E61FEBC
SHA1:	F56F574DAF50D609526B36B5B54FDD59EA4D6A26
SHA-256:	730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A
SHA-512:	D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F AEA
Malicious:	false
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/AccountsService/users/gdm.L6DWB1	
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

/var/lib/AccountsService/users/gdm.L6DWB1	
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/gdm3/.cache/gdm/Xauthority	
Process:	/usr/lib/gdm3/gdm-x-session
File Type:	X11 Xauthority data
Category:	dropped
Size (bytes):	104
Entropy (8bit):	4.995267022754993
Encrypted:	false
SSDEEP:	3:rg/WFllasO93IAw1xj9CzWFllasO93IAw1xj9Cn:rg/WFl2iDgzWFl2iDgn
MD5:	9463654AABC9DA2E12986D5EF5A33407
SHA1:	F04830C284CD99DEBAB239523E3DE4FBE6AB006F
SHA-256:	8FD2D053207688094B93C01C0E948E660A42A43EFE20E70170D96EA28BB0FAFE
SHA-512:	BD7F0016167294224B2E9B495F5BC1A03E2CB0CB79F089FE9DACE943B68F293BD2D9B7E322D64DB77A311C198FE22735031046DAAC98B9A25899D6FF7E22BB0 5
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1..u.).X.yZ.....'....galassia....MIT-MAGIC-COOKIE-1..u.).X.yZ.....'

/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:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE0 9
Malicious:	false
Preview:	.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE0 9
Malicious:	false
Preview:	.

/var/log/Xorg.0.log	
Process:	/usr/lib/xorg/Xorg
File Type:	ASCII text
Category:	dropped
Size (bytes):	41599
Entropy (8bit):	5.290403336903476
Encrypted:	false
SSDEEP:	384:G2pawuQIjNjM6djdNdDdWdHd8dydid5d6dfd3dbdEdWdFdzd2edkd+d/KdGkdXvk:DpaphjesVVd6lS4/WtSIK6Dntu
MD5:	E0E50109E394813F20CE82FFC6B90895
SHA1:	26DE09258ED14D7F65D56243CB7FE54F4441ED73
SHA-256:	E375DBCA46F572C7C1EA09CB0DB8EFAC8B6FCF97792BD2CBAACB3E6106A2ECAD
SHA-512:	8B37E23298DFCA1C4C9C12DA44938B39224843E42D5F3716389BA251A6BA3E91514AC2061F40C22FBD47C7089DFB5E0838616F1AECA059CD773D66E361CFCF5

/var/log/Xorg.0.log	
Malicious:	false
Preview:	[585.042] (--) Log file renamed from "/var/log/Xorg.pid-7095.log" to "/var/log/Xorg.0.log".[585.069] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[5 85.087] Build Operating System: linux Ubuntu.[585.101] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[585.114] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[585.1 57] Build Date: 06 July 2021 10:17:51AM.[585.165] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[585.172] Current version of pixman: 0.38.4.[585.176] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[585.183] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??)

/var/log/wtmp	
Process:	/sbin/agetty
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	0.6775035134351415
Encrypted:	false
SSDEEP:	3:y0sXlXEWtl/DdEPlt:yV+ylZEd
MD5:	6D8C6B9149D531E5C62F920AAD8877A0
SHA1:	CC8B418831FC8A16265DDE0A05BA06EC5177B2A0
SHA-256:	746EC1BBD28F5E3051A1D7595456798685ED355A62EAFDF50C62AC5EDFF06DA4
SHA-512:	DF2D21B795E6CA6091F562CBCFA03D027825E3D9EF623D57FD1533160C2B938A8B97ED58356C00DDF710F23721BBBD25264D8ADA878D881042CFD310B28E6A(B
Malicious:	**true**
Preview:	.....tty2.tty2.....tty2LOGIN.....s.a.%.....

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.446259522251339
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	HgTC70XRum
File size:	73972
MD5:	511762f1b10eab00e1184063857bd215
SHA1:	f51d425c38135a2b7055cf5954afa5837ef5dccf
SHA256:	19818befeeaaa5b480afcac840053c892562a52e948c3d6fc27ea25317dd6776
SHA512:	426e75426d79e14c6097bdc62f8628b6ea114163fc4bf48d9dc1c0b58bd939eb539df25a9c7c0e7e966966a10d879c7df3b6b219dc730fed077091f4b4929a3f
SSDEEP:	1536:rHmydbRaeaCTQztHhEI1GnINTYABxbYCU98CiOa:+hEIclIrYNA
File Content Preview:	.ELF.....D...4...d.....4. ...(.....<...<....T..... .dt.Q.....NV..a....da.....N^NuNV..J9..?$f>"y..<. QJ.g.X.#...<.N."y..<. QJ.f.A.....J.g.Hy....N.X.....?$N^NuNV..N^NuN

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52

ELF header

Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	73572
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x10716	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x800107be	0x107be	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x800107cc	0x107cc	0x1500	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80013cd0	0x11cd0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80013cd8	0x11cd8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80013ce4	0x11ce4	0x240	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80013f24	0x11f24	0x480	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x11f24	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x80000000	0x80000000	0x11ccc	0x11ccc	4.4021	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x11cd0	0x80013cd0	0x80013cd0	0x254	0x6d4	1.7258	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:80
- 192.168.0.14:80

System Behavior

Analysis Process: HgTC70XRum PID: 5247 Parent PID: 5118

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	/tmp/HgTC70XRum
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: HgTC70XRum PID: 5249 Parent PID: 5247

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5251 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5252 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5255 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5258 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5259 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5262 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5263 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HgTC70XRum PID: 5265 Parent PID: 5249

General

Start time:	04:51:53
Start date:	01/11/2021
Path:	/tmp/HgTC70XRum
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5276 Parent PID: 1

General

Start time:	04:51:58
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5276 Parent PID: 1

General

Start time:	04:51:58
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5277 Parent PID: 1

General

Start time:	04:51:59
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5277 Parent PID: 1

General

Start time:	04:51:59
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5292 Parent PID: 1

General

Start time:	04:52:22
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-resolved PID: 5292 Parent PID: 1

General

Start time:	04:52:22
Start date:	01/11/2021
Path:	/lib/systemd/systemd-resolved
Arguments:	/lib/systemd/systemd-resolved
File size:	415968 bytes
MD5 hash:	c93bbc5e20248114c56896451eab7a8b

File Activities

File Deleted

File Read

File Written

Permission Modified

Analysis Process: systemd PID: 5574 Parent PID: 1

General

Start time:	04:52:32
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5574 Parent PID: 1

General

Start time:	04:52:32
Start date:	01/11/2021
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes

MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5709 Parent PID: 1

General

Start time:	04:52:32
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5709 Parent PID: 1

General

Start time:	04:52:32
Start date:	01/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 5724 Parent PID: 5709

General

Start time:	04:52:33
Start date:	01/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 5724 Parent PID: 5709

General

Start time:	04:52:33
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: language-validate PID: 5725 Parent PID: 5724

General

Start time:	04:52:33
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5725 Parent PID: 5724

General

Start time:	04:52:33
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 5726 Parent PID: 5725

General

Start time:	04:52:34
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5726 Parent PID: 5725

General

Start time:	04:52:34
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5727 Parent PID: 5726

General

Start time:	04:52:34
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5727 Parent PID: 5726

General

Start time:	04:52:34
Start date:	01/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5728 Parent PID: 5726

General

Start time:	04:52:34
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5728 Parent PID: 5726

General

Start time:	04:52:34
Start date:	01/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: xfce4-session PID: 5712 Parent PID: 1900

General

Start time:	04:52:32
Start date:	01/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: systemd PID: 5715 Parent PID: 1860

General

Start time:	04:52:32
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5715 Parent PID: 1860

General

Start time:	04:52:32
Start date:	01/11/2021

Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gdm-session-worker PID: 5721 Parent PID: 1809

General

Start time:	04:52:33
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: Default PID: 5721 Parent PID: 1809

General

Start time:	04:52:33
Start date:	01/11/2021
Path:	/etc/gdm3/PostSession/Default
Arguments:	/etc/gdm3/PostSession/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5733 Parent PID: 1320

General

Start time:	04:52:35
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5733 Parent PID: 1320

General

Start time:	04:52:35
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm-session-worker PID: 5740 Parent PID: 5733

General

Start time:	04:52:37
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 5740 Parent PID: 5733

General

Start time:	04:52:37
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	/usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

File Read

File Written

Directory Created

Analysis Process: gdm-x-session PID: 5742 Parent PID: 5740

General

Start time:	04:52:38
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes

MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: Xorg PID: 5742 Parent PID: 5740

General

Start time:	04:52:38
Start date:	01/11/2021
Path:	/usr/bin/Xorg
Arguments:	/usr/bin/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: Xorg.wrap PID: 5742 Parent PID: 5740

General

Start time:	04:52:38
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg.wrap
Arguments:	/usr/lib/xorg/Xorg.wrap vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	14488 bytes
MD5 hash:	48993830888200ecf19dd7def0884dfd

File Activities

File Read

Analysis Process: Xorg PID: 5742 Parent PID: 5740

General

Start time:	04:52:38
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	/usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/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: 5753 Parent PID: 5742

General

Start time:	04:52:45
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5753 Parent PID: 5742

General

Start time:	04:52:45
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5754 Parent PID: 5753

General

Start time:	04:52:45
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5754 Parent PID: 5753

General

Start time:	04:52:45
Start date:	01/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: gdm-x-session PID: 5774 Parent PID: 5740

General

Start time:	04:52:50
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 5774 Parent PID: 5740

General

Start time:	04:52:50
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --print-address 4 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5778 Parent PID: 5774

General

Start time:	04:52:51
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5779 Parent PID: 5778

General

Start time:	04:52:51

Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5779 Parent PID: 5778

General

Start time:	04:52:51
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: gdm3 PID: 5736 Parent PID: 1320

General

Start time:	04:52:36
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5736 Parent PID: 1320

General

Start time:	04:52:36
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5737 Parent PID: 1320

General

Start time:	04:52:36
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5737 Parent PID: 1320

General

Start time:	04:52:36
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5738 Parent PID: 1320

General

Start time:	04:52:36
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5738 Parent PID: 1320

General

Start time:	04:52:36
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5780 Parent PID: 1320

General

Start time:	04:52:52
Start date:	01/11/2021
Path:	/usr/sbin/gdm3

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

Analysis Process: Default PID: 5780 Parent PID: 1320

General

Start time:	04:52:52
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5781 Parent PID: 1320

General

Start time:	04:52:52
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5781 Parent PID: 1320

General

Start time:	04:52:52
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5828 Parent PID: 1

General

Start time:	04:54:02
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5828 Parent PID: 1

General

Start time:	04:54:02
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5831 Parent PID: 1

General

Start time:	04:54:03
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-resolved PID: 5831 Parent PID: 1

General

Start time:	04:54:03
Start date:	01/11/2021
Path:	/lib/systemd/systemd-resolved
Arguments:	/lib/systemd/systemd-resolved
File size:	415968 bytes
MD5 hash:	c93bbc5e20248114c56896451eab7a8b

File Activities

File Deleted

File Read

File Written

Permission Modified

Analysis Process: systemd PID: 5847 Parent PID: 1

General

Start time:	04:54:02
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5847 Parent PID: 1

General

Start time:	04:54:02
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 6095 Parent PID: 1

General

Start time:	04:54:04
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 6095 Parent PID: 1

General

Start time:	04:54:04
Start date:	01/11/2021
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 6214 Parent PID: 1

General

Start time:	04:54:05
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 6214 Parent PID: 1

General

Start time:	04:54:05
Start date:	01/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 6220 Parent PID: 6214

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 6220 Parent PID: 6214

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: language-validate PID: 6221 Parent PID: 6220

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 6221 Parent PID: 6220

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 6222 Parent PID: 6221

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options

Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 6222 Parent PID: 6221

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 6223 Parent PID: 6222

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 6223 Parent PID: 6222

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6224 Parent PID: 6222

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/bin/sh

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

Analysis Process: grep PID: 6224 Parent PID: 6222

General

Start time:	04:54:06
Start date:	01/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gdm3 PID: 6225 Parent PID: 1320

General

Start time:	04:54:08
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 6225 Parent PID: 1320

General

Start time:	04:54:08
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm-session-worker PID: 6240 Parent PID: 6225

General

Start time:	04:54:10

Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 6240 Parent PID: 6225

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	/usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

File Read

File Written

Directory Created

Analysis Process: gdm-x-session PID: 6242 Parent PID: 6240

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: Xorg PID: 6242 Parent PID: 6240

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/bin/Xorg
Arguments:	/usr/bin/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: Xorg.wrap PID: 6242 Parent PID: 6240

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg.wrap
Arguments:	/usr/lib/xorg/Xorg.wrap vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	14488 bytes
MD5 hash:	48993830888200ecf19dd7def0884dfd

File Activities

File Read

Analysis Process: Xorg PID: 6242 Parent PID: 6240

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	/usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /var/lib/gdm3/.cache/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: 6429 Parent PID: 6242

General

Start time:	04:54:25
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 6429 Parent PID: 6242

General

Start time:	04:54:25
Start date:	01/11/2021

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

File Activities

File Read

Analysis Process: sh PID: 6506 Parent PID: 6429

General

Start time:	04:54:26
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 6506 Parent PID: 6429

General

Start time:	04:54:26
Start date:	01/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: gdm-x-session PID: 6678 Parent PID: 6240

General

Start time:	04:54:32
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 6678 Parent PID: 6240

General

Start time:	04:54:32
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --print-address 4 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 6680 Parent PID: 6678

General

Start time:	04:54:34
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 6681 Parent PID: 6680

General

Start time:	04:54:34
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 6681 Parent PID: 6680

General

Start time:	04:54:34
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: systemd PID: 6231 Parent PID: 1

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 6231 Parent PID: 1

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	/lib/systemd/systemd --user
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Directory Deleted

Symbolic Link Created

Analysis Process: systemd PID: 6243 Parent PID: 6231

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 6244 Parent PID: 6243

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: 30-systemd-environment-d-generator PID: 6244 Parent PID: 6243

General

Start time:	04:54:10
Start date:	01/11/2021
Path:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
Arguments:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
File size:	14480 bytes
MD5 hash:	42417da8051ba8ee0eea7854c62d99ca

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 6251 Parent PID: 6231

General

Start time:	04:54:16
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemctl PID: 6251 Parent PID: 6231

General

Start time:	04:54:16
Start date:	01/11/2021
Path:	/bin/systemctl
Arguments:	/bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: systemd PID: 6252 Parent PID: 6231

General

Start time:	04:54:16
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: pulseaudio PID: 6252 Parent PID: 6231

General

Start time:	04:54:18
Start date:	01/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 6267 Parent PID: 1

General

Start time:	04:54:26
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-resolved PID: 6267 Parent PID: 1

General

Start time:	04:54:26
Start date:	01/11/2021
Path:	/lib/systemd/systemd-resolved
Arguments:	/lib/systemd/systemd-resolved
File size:	415968 bytes
MD5 hash:	c93bbc5e20248114c56896451eab7a8b

File Activities

File Deleted

File Read

File Written

Permission Modified

Analysis Process: systemd PID: 6552 Parent PID: 1

General

Start time:	04:54:26
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 6552 Parent PID: 1

General

Start time:	04:54:26
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 6555 Parent PID: 1

General

Start time:	04:54:28
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 6555 Parent PID: 1

General

Start time:	04:54:28
Start date:	01/11/2021
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 6672 Parent PID: 1

General

Start time:	04:54:28
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 6672 Parent PID: 1

General

Start time:	04:54:28
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm3 PID: 6675 Parent PID: 1320

General

Start time:	04:54:31
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 6675 Parent PID: 1320

General

Start time:	04:54:31
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 6676 Parent PID: 1320

General

Start time:	04:54:31
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 6676 Parent PID: 1320

General

Start time:	04:54:31
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 6690 Parent PID: 1

General

Start time:	04:54:40
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-resolved PID: 6690 Parent PID: 1

General

Start time:	04:54:40
Start date:	01/11/2021
Path:	/lib/systemd/systemd-resolved
Arguments:	/lib/systemd/systemd-resolved
File size:	415968 bytes
MD5 hash:	c93bbc5e20248114c56896451eab7a8b

File Activities

File Deleted

File Read

File Written

Permission Modified

Analysis Process: systemd PID: 6953 Parent PID: 1

General

Start time:	04:54:40
Start date:	01/11/2021

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

Analysis Process: systemd-logind PID: 6953 Parent PID: 1

General

Start time:	04:54:40
Start date:	01/11/2021
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 7072 Parent PID: 1

General

Start time:	04:54:41
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 7072 Parent PID: 1

General

Start time:	04:54:41
Start date:	01/11/2021
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \\u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

File Activities

File Read

File Written

Owner / Group Modified

Permission Modified

Analysis Process: systemd PID: 7073 Parent PID: 1

General

Start time:	04:54:41
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 7073 Parent PID: 1

General

Start time:	04:54:41
Start date:	01/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 7078 Parent PID: 7073

General

Start time:	04:54:42
Start date:	01/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 7078 Parent PID: 7073

General

Start time:	04:54:42
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: language-validate PID: 7079 Parent PID: 7078

General

Start time:	04:54:42
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 7079 Parent PID: 7078

General

Start time:	04:54:42
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 7080 Parent PID: 7079

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/share/language-tools/language-options

Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 7080 Parent PID: 7079

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 7081 Parent PID: 7080

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 7081 Parent PID: 7080

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 7083 Parent PID: 7080

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/bin/sh

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

Analysis Process: grep PID: 7083 Parent PID: 7080

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 7077 Parent PID: 1

General

Start time:	04:54:41
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 7077 Parent PID: 1

General

Start time:	04:54:41
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 7082 Parent PID: 1

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd

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

Analysis Process: sshd PID: 7082 Parent PID: 1

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm3 PID: 7084 Parent PID: 1320

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 7084 Parent PID: 1320

General

Start time:	04:54:43
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm-session-worker PID: 7092 Parent PID: 7084

General

Start time:	04:54:46
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 7092 Parent PID: 7084

General

Start time:	04:54:46
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	/usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

File Read

File Written

Directory Created

Analysis Process: gdm-x-session PID: 7095 Parent PID: 7092

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: Xorg PID: 7095 Parent PID: 7092

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/usr/bin/Xorg
Arguments:	/usr/bin/Xorg vt3 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: Xorg.wrap PID: 7095 Parent PID: 7092

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg.wrap
Arguments:	/usr/lib/xorg/Xorg.wrap vt3 -displayfd 3 -auth /var/lib/gdm3/.cache/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	14488 bytes
MD5 hash:	48993830888200ecf19dd7def0884dfd

File Activities

File Read

Analysis Process: Xorg PID: 7095 Parent PID: 7092

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	/usr/lib/xorg/Xorg vt3 -displayfd 3 -auth /var/lib/gdm3/.cache/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: 7497 Parent PID: 7095

General

Start time:	04:55:01
Start date:	01/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 7497 Parent PID: 7095

General

Start time:	04:55:01
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 7498 Parent PID: 7497

General

Start time:	04:55:01
Start date:	01/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 7498 Parent PID: 7497

General

Start time:	04:55:01
Start date:	01/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: gdm-x-session PID: 7500 Parent PID: 7092

General

Start time:	04:55:05
Start date:	01/11/2021
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a
File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 7500 Parent PID: 7092

General

Start time:	04:55:05
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	dbus-daemon --print-address 4 --session
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 7502 Parent PID: 7500

General

Start time:	04:55:05
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 7503 Parent PID: 7502

General

Start time:	04:55:05
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: false PID: 7503 Parent PID: 7502

General

Start time:	04:55:05
Start date:	01/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

Analysis Process: systemd PID: 7088 Parent PID: 1

General

Start time:	04:54:45
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd

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

Analysis Process: systemd PID: 7088 Parent PID: 1

General

Start time:	04:54:45
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	/lib/systemd/systemd --user
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 7094 Parent PID: 7088

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 7096 Parent PID: 7094

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: 30-systemd-environment-d-generator PID: 7096 Parent PID: 7094

General

Start time:	04:54:47
Start date:	01/11/2021
Path:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
Arguments:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
File size:	14480 bytes
MD5 hash:	42417da8051ba8ee0eea7854c62d99ca

Analysis Process: systemd PID: 7483 Parent PID: 7088

General

Start time:	04:54:55

Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemctl PID: 7483 Parent PID: 7088

General

Start time:	04:54:55
Start date:	01/11/2021
Path:	/bin/systemctl
Arguments:	/bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

Analysis Process: systemd PID: 7486 Parent PID: 7088

General

Start time:	04:54:55
Start date:	01/11/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 7486 Parent PID: 7088

General

Start time:	04:54:56
Start date:	01/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 7101 Parent PID: 1

General

Start time:	04:54:51
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-resolved PID: 7101 Parent PID: 1

General

Start time:	04:54:51
Start date:	01/11/2021
Path:	/lib/systemd/systemd-resolved
Arguments:	/lib/systemd/systemd-resolved
File size:	415968 bytes
MD5 hash:	c93bbc5e20248114c56896451eab7a8b

Analysis Process: systemd PID: 7366 Parent PID: 1

General

Start time:	04:54:52
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 7366 Parent PID: 1

General

Start time:	04:54:52
Start date:	01/11/2021
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

Analysis Process: systemd PID: 7484 Parent PID: 1

General

Start time:	04:54:55
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 7484 Parent PID: 1

General

Start time:	04:54:55
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

Analysis Process: systemd PID: 7485 Parent PID: 1

General

Start time:	04:54:55
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 7485 Parent PID: 1

General

Start time:	04:54:55
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

Analysis Process: gdm3 PID: 7489 Parent PID: 1320

General

Start time:	04:54:56
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 7489 Parent PID: 1320

General

Start time:	04:54:56
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 7490 Parent PID: 1320

General

Start time:	04:54:56
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 7490 Parent PID: 1320

General

Start time:	04:54:56
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c