ID: 528748
Sample Name: seWzsbHlCC
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 18:28:37
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

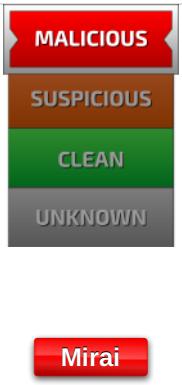
Linux Analysis Report seWzsbHlCC

Overview

General Information

Sample Name:	seWzsbHlCC
Analysis ID:	528748
MD5:	4a3e4fcf840711d..
SHA1:	1debbe3bda8a84..
SHA256:	8797bac4f4912bf..
Tags:	32 arm elf mirai
Infos:	

Detection

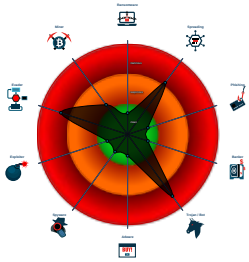


Score:	88
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Sample tries to kill many processes...
- Deletes all firewall rules
- Connects to many ports of the same...
- Sample deletes itself
- Sample is packed with UPX
- Uses known network protocols on no...
- Deletes security-related log files
- Sample reads /proc/mounts (often u...
- Executes the "kill" or "pkill" comman...

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528748
Start date:	25.11.2021
Start time:	18:28:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	seWzsbHlCC
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:	mal88.spre.troj.evad.lin@0/9@2/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- seWzsbHlCC (PID: 5271, Parent: 5122, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/seWzsbHlCC
  - seWzsbHlCC New Fork (PID: 5273, Parent: 5271)
  - seWzsbHlCC New Fork (PID: 5275, Parent: 5271)
    - seWzsbHlCC New Fork (PID: 5278, Parent: 5275)
    - seWzsbHlCC New Fork (PID: 5280, Parent: 5275)
      - seWzsbHlCC New Fork (PID: 5282, Parent: 5280)

- seWzsbHlCC New Fork (PID: 5284, Parent: 5282)
  - sh (PID: 5284, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
    - sh New Fork (PID: 5286, Parent: 5284)
      - rm (PID: 5286, Parent: 5284, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/seWzsbHlCC /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-lofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jlxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
- seWzsbHlCC New Fork (PID: 5293, Parent: 5282)
  - sh (PID: 5293, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /var/log/wtmp"
    - sh New Fork (PID: 5295, Parent: 5293)
      - rm (PID: 5295, Parent: 5293, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
- seWzsbHlCC New Fork (PID: 5296, Parent: 5282)
  - sh (PID: 5296, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/*"
    - sh New Fork (PID: 5298, Parent: 5296)
      - rm (PID: 5298, Parent: 5296, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
- seWzsbHlCC New Fork (PID: 5299, Parent: 5282)
  - sh (PID: 5299, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /bin/netstat"
    - sh New Fork (PID: 5301, Parent: 5299)
      - rm (PID: 5301, Parent: 5299, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
- seWzsbHlCC New Fork (PID: 5302, Parent: 5282)
  - sh (PID: 5302, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -F"
    - sh New Fork (PID: 5304, Parent: 5302)
      - iptables (PID: 5304, Parent: 5302, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -F
- seWzsbHlCC New Fork (PID: 5308, Parent: 5282)
  - sh (PID: 5308, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 busybox"
    - sh New Fork (PID: 5310, Parent: 5308)
      - pkill (PID: 5310, Parent: 5308, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
- seWzsbHlCC New Fork (PID: 5317, Parent: 5282)
  - sh (PID: 5317, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 perl"
    - sh New Fork (PID: 5319, Parent: 5317)
      - pkill (PID: 5319, Parent: 5317, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
- seWzsbHlCC New Fork (PID: 5320, Parent: 5282)
  - sh (PID: 5320, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 python"
    - sh New Fork (PID: 5322, Parent: 5320)
      - pkill (PID: 5322, Parent: 5320, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
- seWzsbHlCC New Fork (PID: 5325, Parent: 5282)
  - sh (PID: 5325, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service iptables stop"
    - sh New Fork (PID: 5327, Parent: 5325)
      - service (PID: 5327, Parent: 5325, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service iptables stop
        - service New Fork (PID: 5328, Parent: 5327)
          - basename (PID: 5328, Parent: 5327, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5329, Parent: 5327)
          - basename (PID: 5329, Parent: 5327, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5330, Parent: 5327)
          - systemctl (PID: 5330, Parent: 5327, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
        - service New Fork (PID: 5331, Parent: 5327)
          - service New Fork (PID: 5332, Parent: 5331)
            - systemctl (PID: 5332, Parent: 5331, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
          - service New Fork (PID: 5333, Parent: 5331)
            - sed (PID: 5333, Parent: 5331, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
      - systemctl (PID: 5327, Parent: 5325, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop iptables.service
- seWzsbHlCC New Fork (PID: 5334, Parent: 5282)
  - sh (PID: 5334, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "/sbin/iptables -F; /sbin/iptables -X"
    - sh New Fork (PID: 5336, Parent: 5334)
      - iptables (PID: 5336, Parent: 5334, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -F
    - sh New Fork (PID: 5337, Parent: 5334)
      - iptables (PID: 5337, Parent: 5334, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -X
- seWzsbHlCC New Fork (PID: 5338, Parent: 5282)
  - sh (PID: 5338, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service firewalld stop"
    - sh New Fork (PID: 5340, Parent: 5338)
      - service (PID: 5340, Parent: 5338, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service firewalld stop
        - service New Fork (PID: 5341, Parent: 5340)
          - basename (PID: 5341, Parent: 5340, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5342, Parent: 5340)
          - basename (PID: 5342, Parent: 5340, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5343, Parent: 5340)
          - systemctl (PID: 5343, Parent: 5340, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
        - service New Fork (PID: 5344, Parent: 5340)
          - service New Fork (PID: 5345, Parent: 5344)
            - systemctl (PID: 5345, Parent: 5344, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
          - service New Fork (PID: 5346, Parent: 5344)
            - sed (PID: 5346, Parent: 5344, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
      - systemctl (PID: 5340, Parent: 5338, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop firewalld.service
- seWzsbHlCC New Fork (PID: 5349, Parent: 5282)
  - sh (PID: 5349, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf ~/.bash_history"
    - sh New Fork (PID: 5351, Parent: 5349)
      - rm (PID: 5351, Parent: 5349, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /root/.bash_history

- seWzsbHlCC New Fork (PID: 5352, Parent: 5282)
- sh (PID: 5352, Parent: 5282, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "history -c"

- systemd New Fork (PID: 5382, Parent: 1)
- whoopsie (PID: 5382, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5407, Parent: 1)
- sshd (PID: 5407, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5408, Parent: 1)
- sshd (PID: 5408, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5413, Parent: 1320)
- Default (PID: 5413, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5414, Parent: 1320)
- Default (PID: 5414, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5417, Parent: 1)
- accounts-daemon (PID: 5417, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
- systemd New Fork (PID: 5446, Parent: 1860)
- pulseaudio (PID: 5446, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5471, Parent: 1)
- gpu-manager (PID: 5471, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5472, Parent: 5471)
  - sh (PID: 5472, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5473, Parent: 5472)
    - grep (PID: 5473, Parent: 5472, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5474, Parent: 5471)
  - sh (PID: 5474, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5475, Parent: 5474)
    - grep (PID: 5475, Parent: 5474, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
  - gpu-manager New Fork (PID: 5476, Parent: 5471)
  - sh (PID: 5476, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5477, Parent: 5476)
    - grep (PID: 5477, Parent: 5476, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5478, Parent: 5471)
  - sh (PID: 5478, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5479, Parent: 5478)
    - grep (PID: 5479, Parent: 5478, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
  - gpu-manager New Fork (PID: 5480, Parent: 5471)
  - sh (PID: 5480, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5481, Parent: 5480)
    - grep (PID: 5481, Parent: 5480, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5482, Parent: 5471)
  - sh (PID: 5482, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5483, Parent: 5482)
    - grep (PID: 5483, Parent: 5482, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
  - gpu-manager New Fork (PID: 5484, Parent: 5471)
  - sh (PID: 5484, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5485, Parent: 5484)
    - grep (PID: 5485, Parent: 5484, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5486, Parent: 5471)
  - sh (PID: 5486, Parent: 5471, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5487, Parent: 5486)
    - grep (PID: 5487, Parent: 5486, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- systemd New Fork (PID: 5488, Parent: 1)
- generate-config (PID: 5488, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5489, Parent: 5488)
  - pkill (PID: 5489, Parent: 5488, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5492, Parent: 1)
- gdm-wait-for-drm (PID: 5492, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- gvfsd-fuse New Fork (PID: 5494, Parent: 2038)
- fusermount (PID: 5494, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5502, Parent: 1)
- systemd-user-runtime-dir (PID: 5502, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5510, Parent: 1)
- gdm3 (PID: 5510, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- systemd New Fork (PID: 5554, Parent: 1)
- gpu-manager (PID: 5554, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5555, Parent: 5554)
  - sh (PID: 5555, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5556, Parent: 5555)
    - grep (PID: 5556, Parent: 5555, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
  - gpu-manager New Fork (PID: 5557, Parent: 5554)
  - sh (PID: 5557, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5558, Parent: 5557)

- grep (PID: 5558, Parent: 5557, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- gpu-manager New Fork (PID: 5559, Parent: 5554)
- sh (PID: 5559, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5560, Parent: 5559)
  - grep (PID: 5560, Parent: 5559, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- gpu-manager New Fork (PID: 5561, Parent: 5554)
- sh (PID: 5561, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5562, Parent: 5561)
  - grep (PID: 5562, Parent: 5561, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- gpu-manager New Fork (PID: 5563, Parent: 5554)
- sh (PID: 5563, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5564, Parent: 5563)
  - grep (PID: 5564, Parent: 5563, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- gpu-manager New Fork (PID: 5565, Parent: 5554)
- sh (PID: 5565, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5566, Parent: 5565)
  - grep (PID: 5566, Parent: 5565, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- gpu-manager New Fork (PID: 5568, Parent: 5554)
- sh (PID: 5568, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5569, Parent: 5568)
  - grep (PID: 5569, Parent: 5568, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- gpu-manager New Fork (PID: 5570, Parent: 5554)
- sh (PID: 5570, Parent: 5554, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5571, Parent: 5570)
  - grep (PID: 5571, Parent: 5570, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- systemd New Fork (PID: 5572, Parent: 1)
- generate-config (PID: 5572, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5573, Parent: 5572)
  - pkill (PID: 5573, Parent: 5572, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5576, Parent: 1)
- gdm-wait-for-drm (PID: 5576, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5582, Parent: 1)
- gdm3 (PID: 5582, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- **cleanup**

Yara Overview

Initial Sample

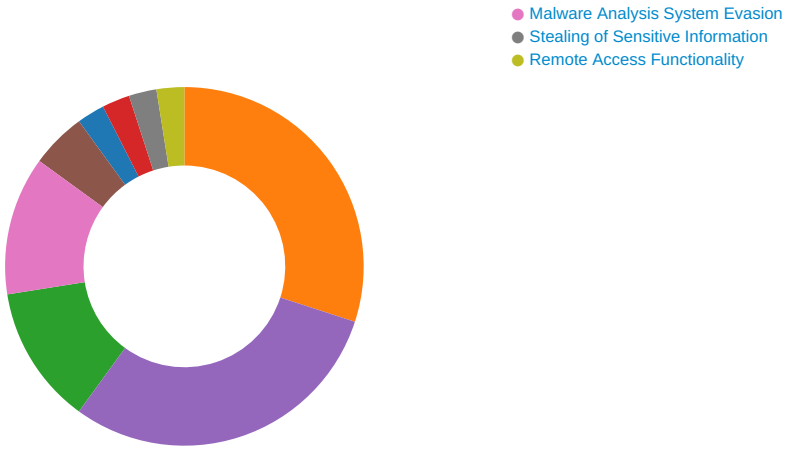
Source	Rule	Description	Author	Strings
seWzsbHlCC	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xb6c8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xb737:$s2: $Id: UPX • 0xb6e8:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Jbx Signature Overview

- Bitcoin Miner
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Deletes all firewall rules
- Connects to many ports of the same IP (likely port scanning)
- Uses known network protocols on non-standard ports

System Summary:

- Sample tries to kill many processes (SIGKILL)

Data Obfuscation:

- Sample is packed with UPX

Persistence and Installation Behavior:

- Deletes all firewall rules
- Sample reads /proc/mounts (often used for finding a writable filesystem)

Hooking and other Techniques for Hiding and Protection:

- Sample deletes itself
- Uses known network protocols on non-standard ports

Malware Analysis System Evasion:

- Deletes security-related log files

Stealing of Sensitive Information:

- Yara detected Mirai

Remote Access Functionality:

- Yara detected Mirai

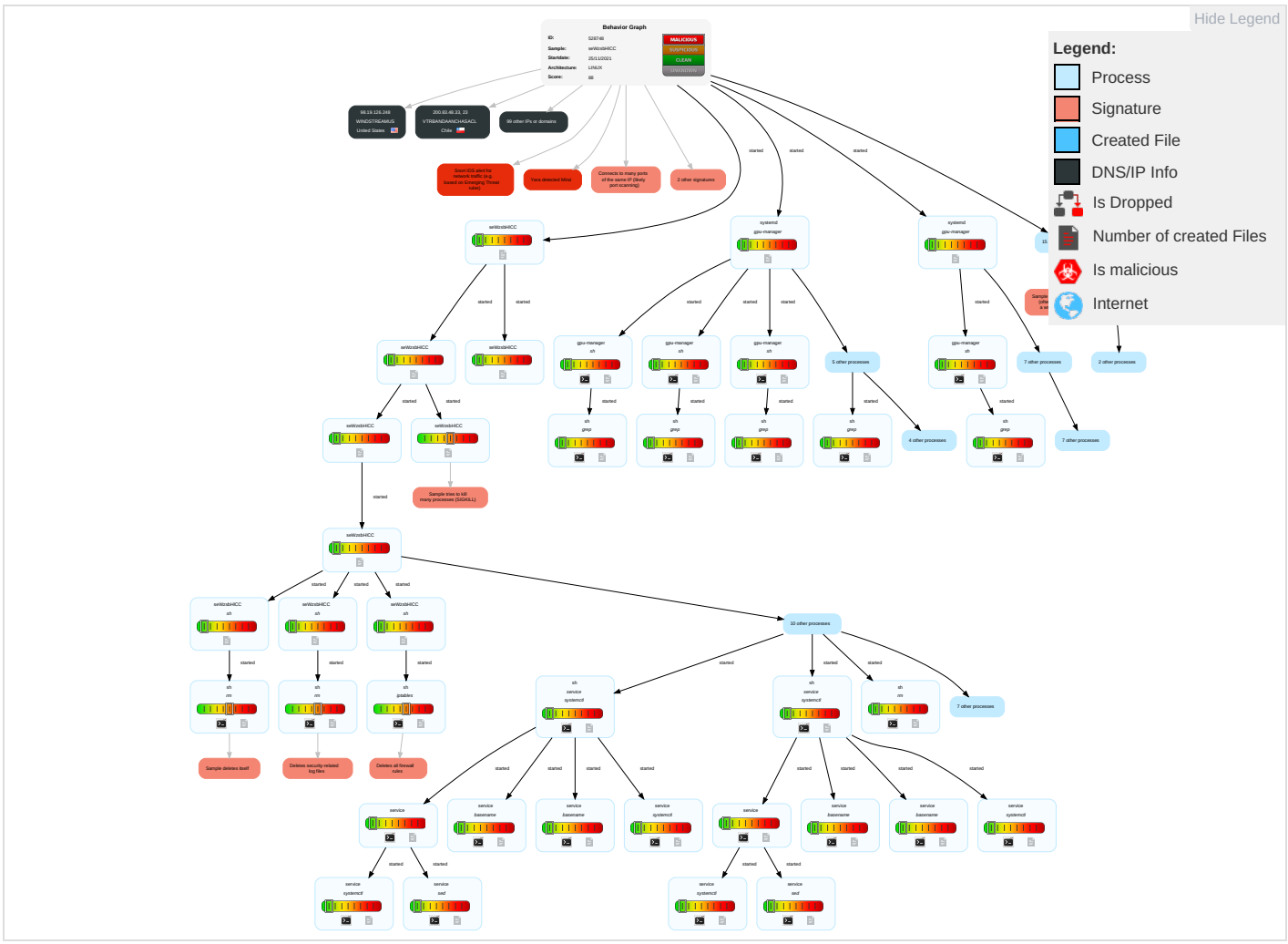
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Path Interception	File and Directory Permissions Modification 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatio
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Network Configuration 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 Authorizatio
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Disable or Modify System Firewall 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Indicator Removal on Host 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
125.42.146.103	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
70.181.35.187	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
207.202.194.215	unknown	United States		2044	IINET-2044US	false
78.161.56.209	unknown	Turkey		9121	TTNETTR	false
1.183.129.29	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
154.157.137.159	unknown	Kenya		36926	CKL1-ASNKE	false
129.140.169.249	unknown	Malawi		37440	Airtel-MW	false
63.198.166.79	unknown	United States		7018	ATT-INTERNET4US	false
181.213.135.162	unknown	Brazil		28573	CLAROSABR	false
190.73.147.200	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
2.93.45.7	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
188.74.238.42	unknown	Romania		60741	MIZA-ASRO	false
37.248.66.119	unknown	Poland		8374	PLUSNETPlusnetworkoperatorinPolandPL	false
151.93.49.118	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
8.28.61.5	unknown	United States		64279	TFSLAOCUS	false
200.83.48.33	unknown	Chile		22047	VTRBANDAANCHASACL	false
155.254.17.225	unknown	United States		397423	TIER-NETUS	false
19.187.8.243	unknown	United States		3	MIT-GATEWAYSUS	false
150.217.104.194	unknown	Italy		137	ASGARRConsortiumGARREU	false
122.105.197.216	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
179.254.251.220	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
98.19.126.248	unknown	United States		7029	WINDSTREAMUS	false
93.87.57.223	unknown	Serbia		8400	TELEKOM-ASRS	false
99.177.214.190	unknown	United States		7018	ATT-INTERNET4US	false
165.139.128.251	unknown	United States		11686	ENAUS	false
47.207.214.207	unknown	United States		5650	FRONTIER-FRTRUS	false
169.97.116.2	unknown	United States		37611	AfrihostZA	false
184.242.62.164	unknown	United States		10507	SPCSUS	false
115.165.146.158	unknown	Japan		9365	ITSCOMitscommunicationsInCJP	false
182.134.184.52	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
86.73.60.242	unknown	France		15557	LDCOMNETFR	false
47.166.238.203	unknown	United States		5650	FRONTIER-FRTRUS	false
216.81.216.18	unknown	United States		11320	LIGHTEDGE-AS-02US	false
110.132.116.231	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
5.127.54.104	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
18.45.73.155	unknown	United States		3	MIT-GATEWAYSUS	false
112.54.85.168	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
174.207.243.210	unknown	United States		22394	CELLCOUS	false
207.48.168.24	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
1.141.94.214	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
206.89.242.95	unknown	United States		3549	LVLT-3549US	false
74.221.73.184	unknown	United States		29979	PWN-ASBLKUS	false
38.83.60.43	unknown	United States		174	COGENT-174US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.161.206.75	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
171.84.126.231	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
112.140.228.143	unknown	Korea Republic of		18318	SPEEDON-AS-KRLGHelloVisionCorpKR	false
166.59.141.111	unknown	United States		3377	MCI-ASNUS	false
20.220.220.250	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
177.201.217.219	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
42.134.246.139	unknown	China		4249	LILLY-ASUS	false
43.11.77.239	unknown	Japan		4249	LILLY-ASUS	false
93.254.32.66	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
35.59.121.11	unknown	United States		36375	UMICH-AS-5US	false
39.223.215.28	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
65.92.251.70	unknown	Canada		577	BACOMCA	false
63.182.214.13	unknown	United States		1239	SPRINTLINKUS	false
135.174.27.61	unknown	United States		14962	NCR-252US	false
124.57.70.69	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
122.32.33.208	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
44.44.171.245	unknown	United States		7377	UCSDUS	false
197.222.122.203	unknown	Egypt		37069	MOBINILEG	false
205.173.0.246	unknown	United States		21633	DOI-NBC-NETUS	false
202.41.22.160	unknown	India		10225	NETTLINX-IN-APNettlinxLimitedIN	false
163.112.152.93	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
19.52.128.103	unknown	United States		3	MIT-GATEWAYSUS	false
57.157.134.55	unknown	Belgium		2686	ATGS-MMD-ASUS	false
210.74.100.133	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
223.216.178.39	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
174.127.145.127	unknown	United States		11404	AS-WAVE-1US	false
203.14.250.15	unknown	Australia		9328	DATACOM-AUDATACOMSYSTEMSAUPTYLTDAU	false
39.85.149.204	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
220.221.217.83	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
32.135.39.52	unknown	United States		2686	ATGS-MMD-ASUS	false
210.115.6.130	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
144.187.229.91	unknown	United States		22562	CSC-IGN-EMEAUS	false
72.46.16.140	unknown	United States		62833	HUDSONFIBERNETUS	false
208.236.99.194	unknown	United States		4208	THE-ISERV-COMPANYUS	false
96.94.23.175	unknown	United States		7922	COMCAST-7922US	false
40.62.7.72	unknown	United States		4249	LILLY-ASUS	false
117.157.129.101	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
58.51.227.57	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
176.83.195.186	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
131.2.49.7	unknown	United States		61458	GOBIERNOAUTONOMOMUNICIPALDELAPAZBO	false
20.130.139.144	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.15.73.68	unknown	United States		7018	ATT-INTERNET4US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.53.48.241	unknown	United States		30722	VODAFONE-IT-ASNIT	false
125.32.16.88	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
134.197.162.8	unknown	United States		3851	NSHE-NEVADANETUS	false
146.181.229.218	unknown	United States		786	JANETJiscServicesLimitedGB	false
78.253.216.102	unknown	France		12322	PROXADFR	false
178.141.254.107	unknown	Russian Federation		44677	MTS-KRV-ASRU	false
108.7.134.33	unknown	United States		701	UUNETUS	false
143.183.65.250	unknown	United States		4983	INTEL-SC-ASUS	false
4.209.69.186	unknown	United States		3356	LEVEL3US	false
187.129.233.71	unknown	Mexico		28283	AdylnetTelecomBR	false
160.120.31.151	unknown	Cote D'ivoire		29571	ORANGE-COTE-IVOIRECI	false
216.227.170.102	unknown	United States		174	COGENT-174US	false
153.47.23.88	unknown	United States		19512	LYONDELLUS	false
205.153.15.235	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
34.99.239.143	unknown	United States		15169	GOOGLEUS	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
151.93.49.118	e4phNkmjAJ	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	arm7-20211121-1750	Get hash	malicious	Browse	• 162.213.33.132
	x86-20211121-1750	Get hash	malicious	Browse	• 162.213.33.132
	arm-20211121-1750	Get hash	malicious	Browse	• 162.213.33.108
	t99LTv3hiB	Get hash	malicious	Browse	• 162.213.33.108
	wPLf38GLbn	Get hash	malicious	Browse	• 162.213.33.132
	E4lCZiGLyr	Get hash	malicious	Browse	• 162.213.33.108
	fYRxyPYc8j	Get hash	malicious	Browse	• 162.213.33.132
	mLh9jwpikq	Get hash	malicious	Browse	• 162.213.33.132
	XLKPMXNVFz	Get hash	malicious	Browse	• 162.213.33.108
	mpsl	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	mips	Get hash	malicious	Browse	• 162.213.33.132
	arm7	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.108
	HFRMJ1PUdK	Get hash	malicious	Browse	• 162.213.33.108
	LPywXJs5AN	Get hash	malicious	Browse	• 162.213.33.132
	Jyw7E6XVyV	Get hash	malicious	Browse	• 162.213.33.132
	YSq7Yxaw94	Get hash	malicious	Browse	• 162.213.33.132
	IJ1I2bAXnS	Get hash	malicious	Browse	• 162.213.33.132
	gEozNq7lLx	Get hash	malicious	Browse	• 162.213.33.132

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	arm7	Get hash	malicious	Browse	• 1.191.108.186
	arm	Get hash	malicious	Browse	• 121.28.150.58
	TDJjjFDkG4	Get hash	malicious	Browse	• 113.230.107.33
	or4ypx7Ery	Get hash	malicious	Browse	• 101.68.23.10
	aljU2bjDwO	Get hash	malicious	Browse	• 119.180.23 3.246
	KEn71AQ430	Get hash	malicious	Browse	• 101.19.160.131

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pwY5ozOzpY	Get hash	malicious	Browse	• 112.132.41.170
	Ljm7n1QDZe	Get hash	malicious	Browse	• 125.44.36.116
	Jx35l5pwgd	Get hash	malicious	Browse	• 61.161.163.133
	HXSFwEhM8m	Get hash	malicious	Browse	• 120.15.222.152
	meerkat.arm7	Get hash	malicious	Browse	• 125.211.65.53
	meerkat.x86	Get hash	malicious	Browse	• 39.82.208.155
	oQANZnrt9d	Get hash	malicious	Browse	• 124.163.22 1.209
	KWDww9OWgh	Get hash	malicious	Browse	• 125.39.128.140
	y8CYO3E0MF	Get hash	malicious	Browse	• 220.192.16 5.211
	Akiru.arm7	Get hash	malicious	Browse	• 121.30.41.210
	Akiru.arm	Get hash	malicious	Browse	• 116.133.14.218
	HLiQSlwlY7	Get hash	malicious	Browse	• 153.7.216.250
	aZsszSGIEV	Get hash	malicious	Browse	• 123.232.160.20
	TwikaSb2s6	Get hash	malicious	Browse	• 115.52.253.248
ASN-CXA-ALL-CCI-22773-RDCUS	l8np4x8FGL	Get hash	malicious	Browse	• 184.186.97.253
	aljU2bjDwO	Get hash	malicious	Browse	• 184.181.23 6.223
	KEn71AQ430	Get hash	malicious	Browse	• 184.185.142.96
	pwY5ozOzpY	Get hash	malicious	Browse	• 98.175.159.215
	Ljm7n1QDZe	Get hash	malicious	Browse	• 174.65.31.255
	Jx35l5pwgd	Get hash	malicious	Browse	• 174.76.96.7
	meerkat.arm7	Get hash	malicious	Browse	• 164.168.23 4.168
	KWDww9OWgh	Get hash	malicious	Browse	• 70.181.35.199
	aZsszSGIEV	Get hash	malicious	Browse	• 98.184.102.0
	sora.x86	Get hash	malicious	Browse	• 68.8.171.134
	NQsLN1nOON	Get hash	malicious	Browse	• 98.187.110.186
	B67M2Q6NeK	Get hash	malicious	Browse	• 98.187.110.188
	c0az1l4js3001lsk4xd9n.arm-20211124-0850	Get hash	malicious	Browse	• 68.0.198.69
	x86_64-20211124-0649	Get hash	malicious	Browse	• 68.109.156.176
	arm-20211124-0649	Get hash	malicious	Browse	• 68.4.59.95
	arm6-20211124-0649	Get hash	malicious	Browse	• 70.178.43.31
	jLvGTP8xik	Get hash	malicious	Browse	• 98.186.255.228
	psl4iJBgiA	Get hash	malicious	Browse	• 98.168.188.216
	zxIlLJKauk	Get hash	malicious	Browse	• 72.212.53.113
	z0r0.x86	Get hash	malicious	Browse	• 24.234.228.113

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

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Reputation:	moderate, very likely benign file
Preview:	auto_null.

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	18
Entropy (8bit):	3.4613201402110088
Encrypted:	false
SSDEEP:	3:5bkrIZsXvn:pkckv
MD5:	28FE6435F34B3367707BB1C5D5F6B430
SHA1:	EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6
SHA-256:	721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0
SHA-512:	6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.monitor.

/proc/5408/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.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:E3v:E3v
MD5:	0BE520D99530BBA5C73589931A7285F6
SHA1:	AB4844E657DB95D0813D4A6947608894835CFF55
SHA-256:	730C50DA4C1A692C53478AAF119272CB220377D13DC420B57D25ACD5BA02BB0A
SHA-512:	B7DB6AAE5EC96AC7CF2B41D7A55B5E32FC5A24FBAABA0C6E829F833C9FDA597DBEFCAEE72E8003B6562EF2A88AC480AF345999497A2B94BE80B8CE8B52DB3312
Malicious:	false
Reputation:	low
Preview:	5408.

/run/systemd/resolve/stub-resolv.conf	
Process:	/tmp/seWzsbHlCC
File Type:	ASCII text
Category:	dropped
Size (bytes):	38
Entropy (8bit):	3.3918926446809334
Encrypted:	false
SSDEEP:	3:KkZRAkd:KaAu

/run/systemd/resolve/stub-resolv.conf	
MD5:	C7EA09D26E26605227076E0514A33038
SHA1:	C3F9736E9AF7BD0885578859A50B205C8FA5FC8E
SHA-256:	7E8AD76E0D200E93918CA2E93C99FF8ECD02071953BF1479819DB3AC0DBB6D07
SHA-512:	17D0088725EB9991E9EB82E8A3DE0878E45E6F394BBC2AD260AA59C786FF0AD565E145E21256425D1C0ABE15F3ECB402EBB0A6A5E1C2D5BA7A4D95EC93A286 1F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	nameserver 8.8.8.8.nameserver 8.8.4.4.

/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:E1v:E1v
MD5:	6E8DD5F0924CE30B35AEAED9C61A5ADD
SHA1:	1208595C4CA7CD0E6980DD4C17DB3965CD6DFBB3
SHA-256:	DC19BDFF69BBF08AFC8FC0C584CBFCD3315D3AAB266D7F97564E71CE74D2774C
SHA-512:	353092740BF752D54D1A451EA5C41A87029B9A5784571F191433028BCDC810D5F4B86493F16C1D83A178776CE5B7B5FE7392B076CD32ECF362C1F2520239539E
Malicious:	false
Reputation:	low
Preview:	5446.

/var/log/gpu-manager.log	
Process:	/usr/bin/gpu-manager
File Type:	ASCII text
Category:	dropped
Size (bytes):	1515
Entropy (8bit):	4.825813629825568
Encrypted:	false
SSDEEP:	24:wPXXX9uV6BNu3WDF3GF3XFFxFFed2uk2HUvJlfWkpPpx7uvvAdow9555Ro7uRkoT:wPXXXe6vejpeC2HUR5WkpPpcvAdow959
MD5:	7B48386106F00126E44F428D0193E1ED
SHA1:	75F652293B2DE03A845A73B678A5CB7E9701A9F4
SHA-256:	9F60B5D0D5C6F6CB3892E1687D16333F36E3BD450713B00FDF0B2BB90EC7312C
SHA-512:	57D0856EC65558B4A843A4696B644AC3E80B3EA0E6EC1C2FAC7A00015B96EBB2CC30967EB8DEFC3E648E59AC6882F6A4F69468D4B6CD0FD60F9F343C206DBF BC
Malicious:	false
Preview:	log_file: /var/log/gpu-manager.log.last_boot_file: /var/lib/ubuntu-drivers-common/last_gfx_boot.new_boot_file: /var/lib/ubuntu-drivers-common/last_gfx_boot.can't access / run/u-d-c-nvidia-was-loaded file.can't get module info via kmodcan't access /opt/amdgpu-pro/bin/amdgpu-pro-px.Looking for nvidia modules in /lib/modules/5.4.0-72- generic/kernel.Looking for nvidia modules in /lib/modules/5.4.0-72-generic/updates/dkms.Looking for amdgpu modules in /lib/modules/5.4.0-72-generic/kernel.Looking for amdgpu modules in /lib/modules/5.4.0-72-generic/updates/dkms.Is nvidia loaded? no.Was nvidia unloaded? no.Is nvidia blacklisted? no.Is intel loaded? no.Is radeon loaded? no.Is radeon blacklisted? no.Is amdgpu loaded? no.Is amdgpu blacklisted? no.Is amdgpu versioned? no.Is amdgpu pro stack? no.Is nouveau loaded? no.Is no uveau blacklisted? no.Is nvidia kernel module available? no.Is amdgpu kernel module available? no.Vendor/Device Id: 15ad:405.BusID "PCI:0@0:15:0".Is boot vga? y es.Error: can't acce

/var/run/gdm3.pid	
Process:	/usr/sbin/gdm3
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:Fd/n:n/n
MD5:	5DE88F8B8A42BF20A95C7C449C13D8DE
SHA1:	42E07D8ECA0D77F8445F835510C1C634DC89E74F
SHA-256:	F9615512F25BC98071A42105AA4A18C4FD1E77EE6B8E7B63B60BAB517DC0114A
SHA-512:	5E1C807B5E7CA6E7A27545BE9418C1954AF3DCA07DE61C9768FCC333A13D646D116DF3B4197B1E106B5C0920DA6FB96FBF83C2F0081937163F22B2FA484661D
Malicious:	false
Preview:	5582.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	7.977062127211769
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	seWzsbHlCC
File size:	48788
MD5:	4a3e4fcf840711d95a782a1aa01a3758
SHA1:	1debbe3bda8a84261eee99edc5f672165a44813d
SHA256:	8797bac4f4912bf412e4dc586f0747c0161de7b3ebd0e680eb814be4e20a7b39
SHA512:	3c978fc2340be0aa980be1302d14d5f9c37c6fc762c1ed579c018410003d45a524f600affca34ebe604a1887e2cf4d186df0836c01d03783a0e2fbee1bf3a6bf
SSDEEP:	768:3UTrAuYC4Ut7wwfhcYIeXrGgkoJBSwrauyOgYfZDAK+/BVZUUMK+P3FKxUOphDl7:3On4Utwch5Gm70/6UL+P3FK6QhR5yz1S
File Content Preview:	.ELF...a.....(.....+..4.....4. ...(.....@o..@o..@o.....Q.td.....t.6.UPX!.....S.....?.E.h;.}...^.....f.+....E.....~.....*.....k.#..^.8.....Nf3p2f.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x12bf8
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0xbda7	0xbda7	4.0364	0x5	R E	0x8000		
LOAD	0x6f40	0x36f40	0x36f40	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:30:11.517456055 CET	192.168.2.23	8.8.8.8	0x808e	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:30:11.518490076 CET	192.168.2.23	8.8.8.8	0xbc8d	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:30:11.549971104 CET	8.8.8.8	192.168.2.23	0x808e	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Nov 25, 2021 18:30:11.549971104 CET	8.8.8.8	192.168.2.23	0x808e	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: seWzsbHlCC PID: 5271 Parent PID: 5122

General

Start time:	18:29:21
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	/tmp/seWzsbHlCC
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: seWzsbHlCC PID: 5273 Parent PID: 5271

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: seWzsbHlCC PID: 5275 Parent PID: 5271

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: seWzsbHlCC PID: 5278 Parent PID: 5275

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: seWzsbHlCC PID: 5280 Parent PID: 5275

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: seWzsbHlCC PID: 5282 Parent PID: 5280

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Written

Analysis Process: seWzsbHlCC PID: 5284 Parent PID: 5282

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5284 Parent PID: 5282

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5286 Parent PID: 5284

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5286 Parent PID: 5284

General

Start time:	18:29:22
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/seWzsbHlCC /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jlxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Directory Enumerated

Analysis Process: seWzsbHICC PID: 5293 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5293 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /var/log/wtmp"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5295 Parent PID: 5293

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5295 Parent PID: 5293

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /var/log/wtmp
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: seWzsbHICC PID: 5296 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5296 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5298 Parent PID: 5296

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5298 Parent PID: 5296

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/*
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: seWzsbHICC PID: 5299 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5299 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /bin/netstat"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5301 Parent PID: 5299

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5301 Parent PID: 5299

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /bin/netstat
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: seWzsbHICC PID: 5302 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5302 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "iptables -F"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5304 Parent PID: 5302

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5304 Parent PID: 5302

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/usr/sbin/iptables
Arguments:	iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: seWzsbHICC PID: 5308 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5308 Parent PID: 5282

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5310 Parent PID: 5308

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5310 Parent PID: 5308

General

Start time:	18:29:34
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 busybox
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: seWzsbHICC PID: 5317 Parent PID: 5282

General

Start time:	18:29:36
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5317 Parent PID: 5282

General

Start time:	18:29:36
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 perl"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5319 Parent PID: 5317

General

Start time:	18:29:36
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5319 Parent PID: 5317

General

Start time:	18:29:36
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 perl
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: seWzsbHICC PID: 5320 Parent PID: 5282

General

Start time:	18:29:38
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5320 Parent PID: 5282

General

Start time:	18:29:38
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 python"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5322 Parent PID: 5320

General

Start time:	18:29:38
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5322 Parent PID: 5320

General

Start time:	18:29:38
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 python
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: seWzsbHICC PID: 5325 Parent PID: 5282

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5325 Parent PID: 5282

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "service iptables stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5327 Parent PID: 5325

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5327 Parent PID: 5325

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	service iptables stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: 5328 Parent PID: 5327

General

Start time:	18:29:41

Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5328 Parent PID: 5327

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5329 Parent PID: 5327

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5329 Parent PID: 5327

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5330 Parent PID: 5327

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5330 Parent PID: 5327

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active multi-user.target
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: service PID: 5331 Parent PID: 5327

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5332 Parent PID: 5331

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5332 Parent PID: 5331

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl list-unit-files --full --type=socket
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Directory Enumerated

Analysis Process: service PID: 5333 Parent PID: 5331

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5333 Parent PID: 5331

General

Start time:	18:29:41
Start date:	25/11/2021
Path:	/usr/bin/sed
Arguments:	sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: systemctl PID: 5327 Parent PID: 5325

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl stop iptables.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: seWzsbHlCC PID: 5334 Parent PID: 5282

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/tmp/seWzsbHlCC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5334 Parent PID: 5282

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "/sbin/iptables -F; /sbin/iptables -X"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5336 Parent PID: 5334

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5336 Parent PID: 5334

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/sbin/iptables
Arguments:	/sbin/iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: sh PID: 5337 Parent PID: 5334

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5337 Parent PID: 5334

General

Start time:	18:29:43
Start date:	25/11/2021
Path:	/sbin/iptables
Arguments:	/sbin/iptables -X
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: seWzsbHICC PID: 5338 Parent PID: 5282

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5338 Parent PID: 5282

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "service firewalld stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5340 Parent PID: 5338

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5340 Parent PID: 5338

General

Start time:	18:29:44

Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	service firewalld stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: 5341 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5341 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5342 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5342 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service

File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5343 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5343 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active multi-user.target
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: service PID: 5344 Parent PID: 5340

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5345 Parent PID: 5344

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5345 Parent PID: 5344

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl list-unit-files --full --type=socket
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Directory Enumerated

Analysis Process: service PID: 5346 Parent PID: 5344

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5346 Parent PID: 5344

General

Start time:	18:29:44
Start date:	25/11/2021
Path:	/usr/bin/sed
Arguments:	sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: systemctl PID: 5340 Parent PID: 5338

General

Start time:	18:29:47
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl stop firewalld.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: seWzsbHICC PID: 5349 Parent PID: 5282

General

Start time:	18:29:47
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5349 Parent PID: 5282

General

Start time:	18:29:47
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf ~/.bash_history"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5351 Parent PID: 5349

General

Start time:	18:29:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5351 Parent PID: 5349

General

Start time:	18:29:48
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /root/.bash_history
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: seWzsbHICC PID: 5352 Parent PID: 5282

General

Start time:	18:29:48
Start date:	25/11/2021
Path:	/tmp/seWzsbHICC
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5352 Parent PID: 5282

General

Start time:	18:29:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "history -c"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5382 Parent PID: 1

General

Start time:	18:30:10
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5382 Parent PID: 1

General

Start time:	18:30:10
Start date:	25/11/2021
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

Directory Enumerated

Directory Created

Owner / Group Modified

Permission Modified

Analysis Process: systemd PID: 5407 Parent PID: 1

General

Start time:	18:30:14
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5407 Parent PID: 1

General

Start time:	18:30:14
Start date:	25/11/2021
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: 5408 Parent PID: 1

General

Start time:	18:30:14
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5408 Parent PID: 1

General

Start time:	18:30:14
Start date:	25/11/2021
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: 5413 Parent PID: 1320

General

Start time:	18:30:21
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5413 Parent PID: 1320

General

Start time:	18:30:21
Start date:	25/11/2021
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: 5414 Parent PID: 1320

General

Start time:	18:30:21
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5414 Parent PID: 1320

General

Start time:	18:30:21

Start date:	25/11/2021
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: 5417 Parent PID: 1

General

Start time:	18:30:21
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5417 Parent PID: 1

General

Start time:	18:30:21
Start date:	25/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

Analysis Process: systemd PID: 5446 Parent PID: 1860

General

Start time:	18:30:43
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5446 Parent PID: 1860

General

Start time:	18:30:43
Start date:	25/11/2021
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: 5471 Parent PID: 1

General

Start time:	18:30:47
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5471 Parent PID: 1

General

Start time:	18:30:47
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

Directory Enumerated

Analysis Process: gpu-manager PID: 5472 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5472 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5473 Parent PID: 5472

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5473 Parent PID: 5472

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5474 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes

MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5474 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5475 Parent PID: 5474

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5475 Parent PID: 5474

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5476 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes

MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5476 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5477 Parent PID: 5476

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5477 Parent PID: 5476

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5478 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager

Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5478 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5479 Parent PID: 5478

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5479 Parent PID: 5478

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5480 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021

Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5480 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5481 Parent PID: 5480

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5481 Parent PID: 5480

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5482 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5482 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5483 Parent PID: 5482

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5483 Parent PID: 5482

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5484 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5484 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5485 Parent PID: 5484

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5485 Parent PID: 5484

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5486 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5486 Parent PID: 5471

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5487 Parent PID: 5486

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5487 Parent PID: 5486

General

Start time:	18:30:48
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5488 Parent PID: 1

General

Start time:	18:30:50
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5488 Parent PID: 1

General

Start time:	18:30:50
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: generate-config PID: 5489 Parent PID: 5488

General

Start time:	18:30:50
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5489 Parent PID: 5488

General

Start time:	18:30:50
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5492 Parent PID: 1

General

Start time:	18:30:52
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5492 Parent PID: 1

General

Start time:	18:30:52
Start date:	25/11/2021
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities

File Read

Directory Enumerated

Analysis Process: gvfsd-fuse PID: 5494 Parent PID: 2038

General

Start time:	18:30:55
Start date:	25/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5494 Parent PID: 2038

General

Start time:	18:30:55
Start date:	25/11/2021
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

File Activities

File Read

Analysis Process: systemd PID: 5502 Parent PID: 1

General

Start time:	18:30:55
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5502 Parent PID: 1

General

Start time:	18:30:55
Start date:	25/11/2021
Path:	/lib/systemd/systemd-user-runtime-dir
Arguments:	/lib/systemd/systemd-user-runtime-dir stop 1000
File size:	22672 bytes
MD5 hash:	d55f4b0847f88131dbcfb07435178e54

File Activities

File Deleted

File Read

Directory Enumerated

Directory Deleted

Analysis Process: systemd PID: 5510 Parent PID: 1

General

Start time:	18:31:02
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5510 Parent PID: 1

General

Start time:	18:31:02
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Deleted

File Read

File Written

Directory Created

Owner / Group Modified

Permission Modified

Analysis Process: systemd PID: 5554 Parent PID: 1

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5554 Parent PID: 1

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Analysis Process: gpu-manager PID: 5555 Parent PID: 5554

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5555 Parent PID: 5554

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5556 Parent PID: 5555

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5556 Parent PID: 5555

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5557 Parent PID: 5554

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5557 Parent PID: 5554

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5558 Parent PID: 5557

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5558 Parent PID: 5557

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5559 Parent PID: 5554

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5559 Parent PID: 5554

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5560 Parent PID: 5559

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5560 Parent PID: 5559

General

Start time:	18:32:33
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5561 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5561 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5562 Parent PID: 5561

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5562 Parent PID: 5561

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5563 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5563 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5564 Parent PID: 5563

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5564 Parent PID: 5563

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5565 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes

MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5565 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5566 Parent PID: 5565

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5566 Parent PID: 5565

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5568 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes

MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5568 Parent PID: 5554

General

Start time:	18:32:34
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5569 Parent PID: 5568

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5569 Parent PID: 5568

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5570 Parent PID: 5554

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager

Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5570 Parent PID: 5554

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5571 Parent PID: 5570

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5571 Parent PID: 5570

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5572 Parent PID: 1

General

Start time:	18:32:35
Start date:	25/11/2021

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

Analysis Process: generate-config PID: 5572 Parent PID: 1

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: generate-config PID: 5573 Parent PID: 5572

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5573 Parent PID: 5572

General

Start time:	18:32:35
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5576 Parent PID: 1

General

Start time:	18:32:37
Start date:	25/11/2021

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

Analysis Process: gdm-wait-for-drm PID: 5576 Parent PID: 1

General

Start time:	18:32:37
Start date:	25/11/2021
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5582 Parent PID: 1

General

Start time:	18:32:47
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5582 Parent PID: 1

General

Start time:	18:32:47
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Deleted

File Read

File Written

Directory Created

Owner / Group Modified

Permission Modified