ID: 519695
Sample Name: arm7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:07:26
Date: 11/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

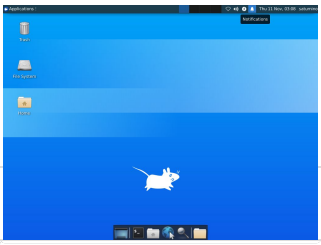
Linux Analysis Report arm7

Overview

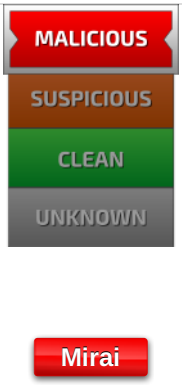
General Information

Sample Name:	arm7
Analysis ID:	519695
MD5:	9fc0975479e319f..
SHA1:	ff77399d8fb7576…
SHA256:	f0c7eb51c588fa5..
Tags:	Mirai
Infos:	

Most interesting Screenshot:



Detection

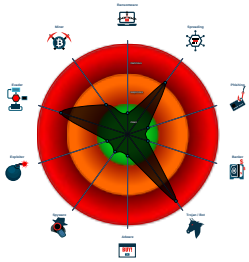


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample tries to kill many processes…
- 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:	519695
Start date:	11.11.2021
Start time:	03:07:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arm7
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.spre.troj.evad.lin@0/9@2/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- arm7 (PID: 5234, Parent: 5112, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm7
  - arm7 New Fork (PID: 5236, Parent: 5234)
  - arm7 New Fork (PID: 5237, Parent: 5234)
  - arm7 New Fork (PID: 5239, Parent: 5234)
  - arm7 New Fork (PID: 5240, Parent: 5234)
  - arm7 New Fork (PID: 5241, Parent: 5234)

- arm7 New Fork (PID: 5245, Parent: 5234)
  - arm7 New Fork (PID: 5249, Parent: 5245)
  - arm7 New Fork (PID: 5251, Parent: 5245)
    - arm7 New Fork (PID: 5253, Parent: 5251)
      - arm7 New Fork (PID: 5255, Parent: 5253)
      - sh (PID: 5255, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
        - sh New Fork (PID: 5257, Parent: 5255)
        - rm (PID: 5257, Parent: 5255, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/arm7 /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /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-1jIxdj /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
      - arm7 New Fork (PID: 5262, Parent: 5253)
      - sh (PID: 5262, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "rm -rf /var/log/wtmp"
        - sh New Fork (PID: 5268, Parent: 5262)
        - rm (PID: 5268, Parent: 5262, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
      - arm7 New Fork (PID: 5269, Parent: 5253)
      - sh (PID: 5269, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "rm -rf /tmp/*"
        - sh New Fork (PID: 5271, Parent: 5269)
        - rm (PID: 5271, Parent: 5269, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
      - arm7 New Fork (PID: 5272, Parent: 5253)
      - sh (PID: 5272, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "rm -rf /bin/netstat"
        - sh New Fork (PID: 5274, Parent: 5272)
        - rm (PID: 5274, Parent: 5272, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
      - arm7 New Fork (PID: 5275, Parent: 5253)
      - sh (PID: 5275, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -F"
        - sh New Fork (PID: 5277, Parent: 5275)
        - iptables (PID: 5277, Parent: 5275, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -F
      - arm7 New Fork (PID: 5281, Parent: 5253)
      - sh (PID: 5281, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "pkill -9 busybox"
        - sh New Fork (PID: 5284, Parent: 5281)
        - pkill (PID: 5284, Parent: 5281, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
      - arm7 New Fork (PID: 5287, Parent: 5253)
      - sh (PID: 5287, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "pkill -9 perl"
        - sh New Fork (PID: 5289, Parent: 5287)
        - pkill (PID: 5289, Parent: 5287, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
      - arm7 New Fork (PID: 5292, Parent: 5253)
      - sh (PID: 5292, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "pkill -9 python"
        - sh New Fork (PID: 5294, Parent: 5292)
        - pkill (PID: 5294, Parent: 5292, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
      - arm7 New Fork (PID: 5295, Parent: 5253)
      - sh (PID: 5295, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "service iptables stop"
        - sh New Fork (PID: 5297, Parent: 5295)
        - service (PID: 5297, Parent: 5295, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service iptables stop
          - service New Fork (PID: 5299, Parent: 5297)
          - basename (PID: 5299, Parent: 5297, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5300, Parent: 5297)
          - basename (PID: 5300, Parent: 5297, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5301, Parent: 5297)
          - systemctl (PID: 5301, Parent: 5297, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
          - service New Fork (PID: 5302, Parent: 5297)
            - service New Fork (PID: 5303, Parent: 5302)
            - systemctl (PID: 5303, Parent: 5302, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
            - service New Fork (PID: 5304, Parent: 5302)
            - sed (PID: 5304, Parent: 5302, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
        - systemctl (PID: 5297, Parent: 5295, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop iptables.service
      - arm7 New Fork (PID: 5308, Parent: 5253)
      - sh (PID: 5308, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "/sbin/iptables -F; /sbin/iptables -X"
        - sh New Fork (PID: 5310, Parent: 5308)
        - iptables (PID: 5310, Parent: 5308, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -F
        - sh New Fork (PID: 5311, Parent: 5308)
        - iptables (PID: 5311, Parent: 5308, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -X
      - arm7 New Fork (PID: 5312, Parent: 5253)
      - sh (PID: 5312, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "service firewalld stop"
        - sh New Fork (PID: 5314, Parent: 5312)
        - service (PID: 5314, Parent: 5312, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service firewalld stop
          - service New Fork (PID: 5315, Parent: 5314)
          - basename (PID: 5315, Parent: 5314, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5316, Parent: 5314)
          - basename (PID: 5316, Parent: 5314, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5317, Parent: 5314)
          - systemctl (PID: 5317, Parent: 5314, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
          - service New Fork (PID: 5318, Parent: 5314)
            - service New Fork (PID: 5319, Parent: 5318)
            - systemctl (PID: 5319, Parent: 5318, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
            - service New Fork (PID: 5320, Parent: 5318)
            - sed (PID: 5320, Parent: 5318, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
        - systemctl (PID: 5314, Parent: 5312, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop firewalld.service

- arm7 New Fork (PID: 5323, Parent: 5253)
  - sh (PID: 5323, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "rm -rf ~/.bash_history"
    - sh New Fork (PID: 5325, Parent: 5323)
    - rm (PID: 5325, Parent: 5323, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /root/.bash_history
- arm7 New Fork (PID: 5326, Parent: 5253)
  - sh (PID: 5326, Parent: 5253, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "history -c"

- systemd New Fork (PID: 5355, Parent: 1)
  - whoopsie (PID: 5355, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5364, Parent: 1)
  - sshd (PID: 5364, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5365, Parent: 1)
  - sshd (PID: 5365, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5370, Parent: 1320)
  - Default (PID: 5370, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5373, Parent: 1320)
  - Default (PID: 5373, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5374, Parent: 1)
  - accounts-daemon (PID: 5374, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
- systemd New Fork (PID: 5403, Parent: 1860)
  - pulseaudio (PID: 5403, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5428, Parent: 1)
  - gpu-manager (PID: 5428, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5429, Parent: 5428)
    - sh (PID: 5429, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5430, Parent: 5429)
      - grep (PID: 5430, Parent: 5429, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5431, Parent: 5428)
    - sh (PID: 5431, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5432, Parent: 5431)
      - grep (PID: 5432, Parent: 5431, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5433, Parent: 5428)
    - sh (PID: 5433, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5434, Parent: 5433)
      - grep (PID: 5434, Parent: 5433, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5435, Parent: 5428)
    - sh (PID: 5435, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5436, Parent: 5435)
      - grep (PID: 5436, Parent: 5435, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5437, Parent: 5428)
    - sh (PID: 5437, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5438, Parent: 5437)
      - grep (PID: 5438, Parent: 5437, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5439, Parent: 5428)
    - sh (PID: 5439, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5440, Parent: 5439)
      - grep (PID: 5440, Parent: 5439, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5441, Parent: 5428)
    - sh (PID: 5441, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5442, Parent: 5441)
      - grep (PID: 5442, Parent: 5441, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5443, Parent: 5428)
    - sh (PID: 5443, Parent: 5428, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
      - sh New Fork (PID: 5444, Parent: 5443)
      - grep (PID: 5444, Parent: 5443, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5445, Parent: 1)
  - generate-config (PID: 5445, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
    - generate-config New Fork (PID: 5446, Parent: 5445)
    - pkill (PID: 5446, Parent: 5445, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5452, Parent: 1)
  - gdm-wait-for-drm (PID: 5452, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- gvfsd-fuse New Fork (PID: 5456, Parent: 2038)
  - fusermount (PID: 5456, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5476, Parent: 1)
  - systemd-user-runtime-dir (PID: 5476, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5500, Parent: 1)
  - gdm3 (PID: 5500, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- systemd New Fork (PID: 5550, Parent: 1)
  - gpu-manager (PID: 5550, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5551, Parent: 5550)
    - sh (PID: 5551, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
      - sh New Fork (PID: 5552, Parent: 5551)
      - grep (PID: 5552, Parent: 5551, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5553, Parent: 5550)
- sh (PID: 5553, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5554, Parent: 5553)
  - grep (PID: 5554, Parent: 5553, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5555, Parent: 5550)
- sh (PID: 5555, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5556, Parent: 5555)
  - grep (PID: 5556, Parent: 5555, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5557, Parent: 5550)
- sh (PID: 5557, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5558, Parent: 5557)
  - grep (PID: 5558, Parent: 5557, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5559, Parent: 5550)
- sh (PID: 5559, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5560, Parent: 5559)
  - grep (PID: 5560, Parent: 5559, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5561, Parent: 5550)
- sh (PID: 5561, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5562, Parent: 5561)
  - grep (PID: 5562, Parent: 5561, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5563, Parent: 5550)
- sh (PID: 5563, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5564, Parent: 5563)
  - grep (PID: 5564, Parent: 5563, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5565, Parent: 5550)
- sh (PID: 5565, Parent: 5550, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5566, Parent: 5565)
  - grep (PID: 5566, Parent: 5565, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5567, Parent: 1)
- generate-config (PID: 5567, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5568, Parent: 5567)
  - pkill (PID: 5568, Parent: 5567, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5569, Parent: 1)
- gdm-wait-for-drm (PID: 5569, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5579, Parent: 1)
- gdm3 (PID: 5579, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
arm7	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xde2c:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xde9b:$s2: $Id: UPX • 0xde4c:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

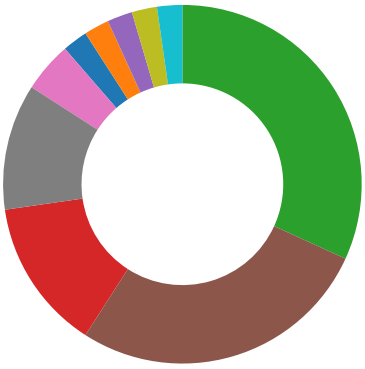
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5241.1.00000000f6abff04.000000008642ee32.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5234.1.00000000f6abff04.000000008642ee32.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5249.1.00000000f6abff04.000000008642ee32.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5236.1.00000000f6abff04.000000008642ee32.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5237.1.00000000f6abff04.000000008642ee32.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Click to see the 5 entries

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

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

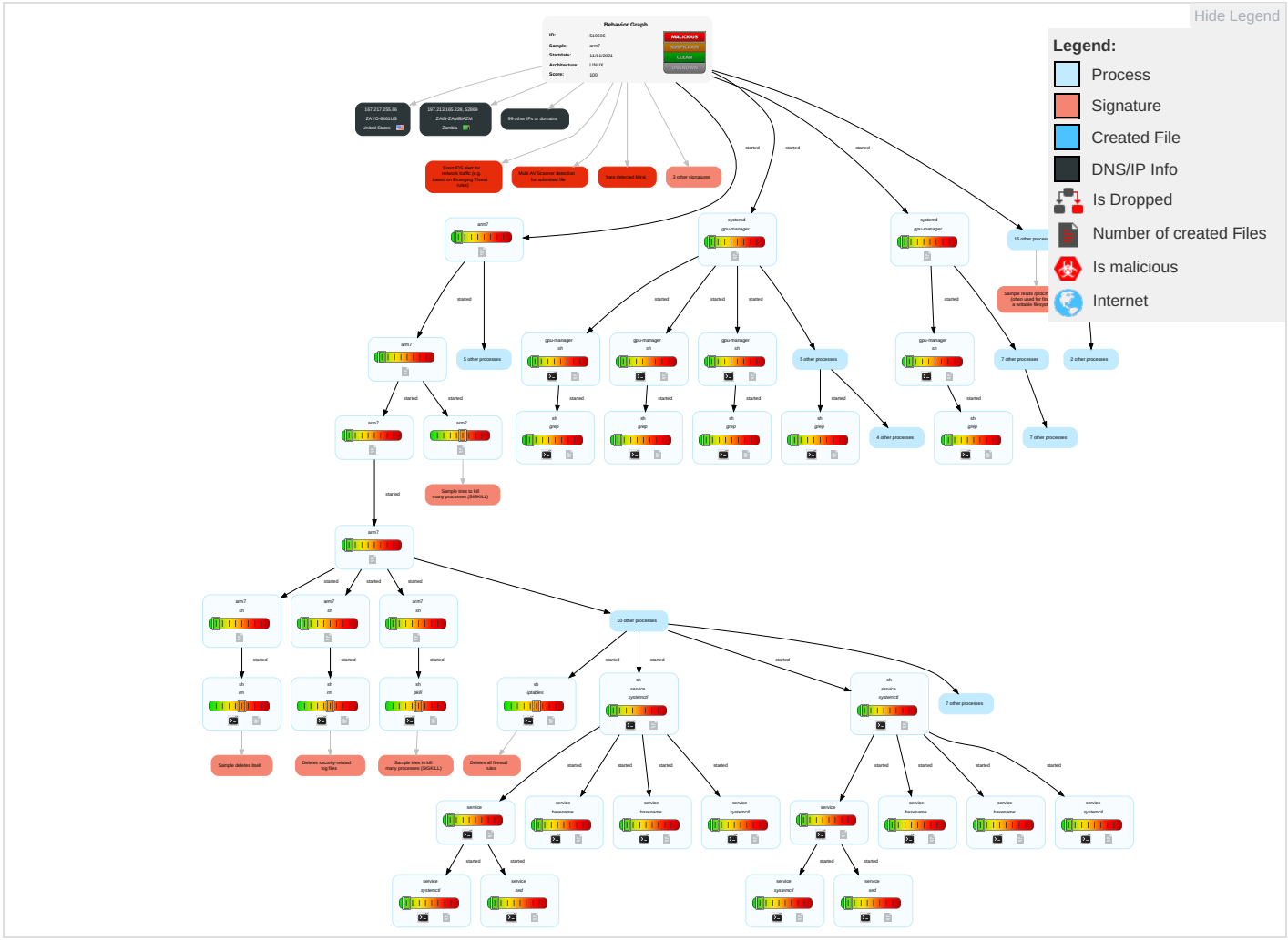
Mitre Att&ck Matrix

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 Device Without Authorization
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 Authorization
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 2	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 3	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

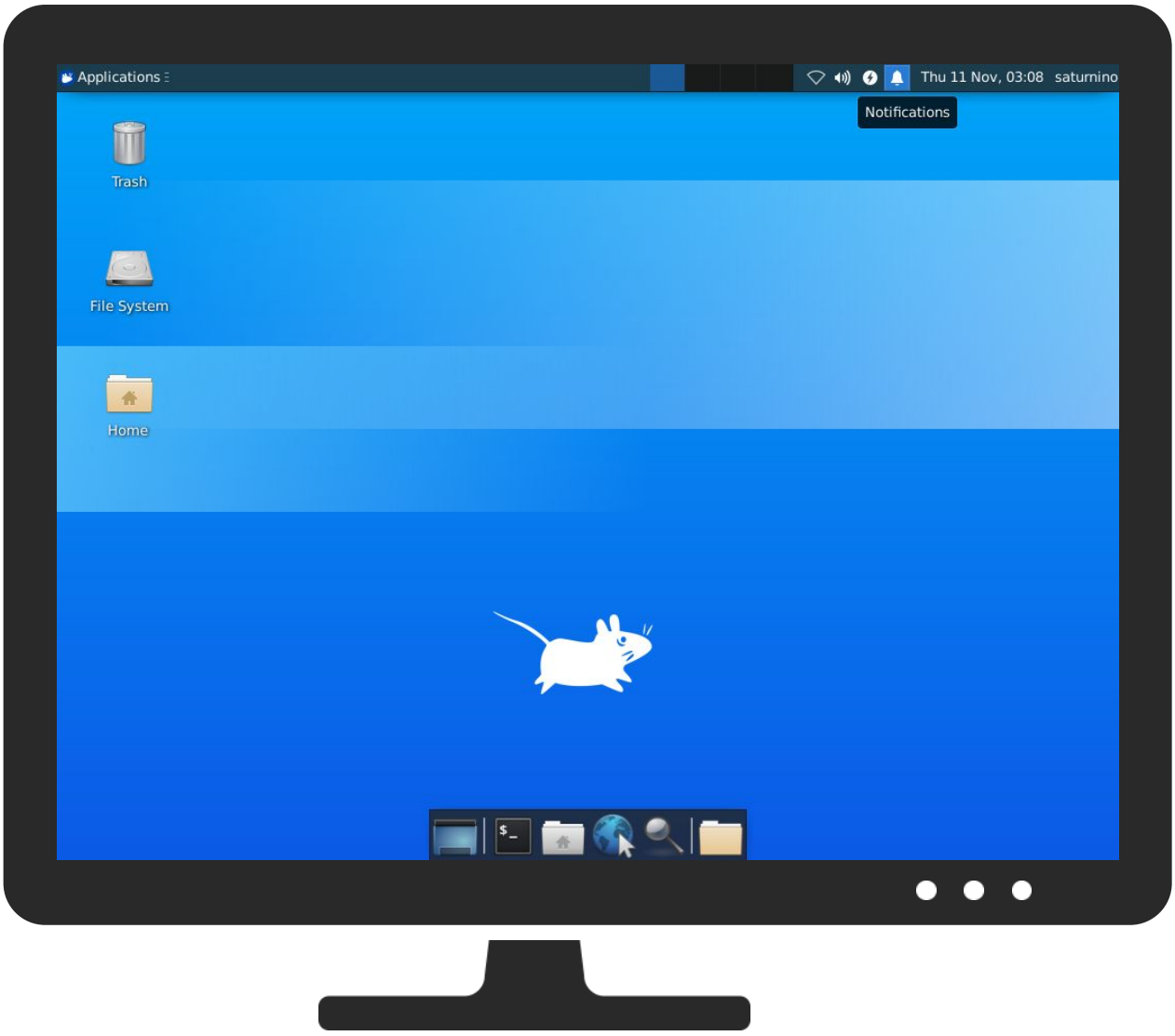
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arm7	23%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://23.94.186.250/..23091t/mips;	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.33.108	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
158.66.163.62	unknown	Poland		21111	CISGCentrumInformacjiSpoleczno-GospodarczejPL	false
208.203.38.141	unknown	United States		701	UUNETUS	false
197.129.211.53	unknown	Morocco		6713	IAM-ASMA	false
132.79.51.81	unknown	United States		306	DNIC-ASBLK-00306-00371US	false
41.108.48.184	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.141.254.118	unknown	United States		29975	VODACOM-ZA	false
156.66.10.209	unknown	United States		29975	VODACOM-ZA	false
144.254.84.93	unknown	United States		109	CISCOSYSTEMSUS	false
156.204.60.88	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.196.170.157	unknown	Egypt		8452	TE-ASTE-ASEG	false
149.184.4.248	unknown	United Kingdom		87	INDIANA-ASUS	false
197.242.86.249	unknown	South Africa		24940	HETZNER-ASDE	false
135.244.53.66	unknown	United States		10455	LUCENT-CIOUS	false
14.105.136.130	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
156.161.229.80	unknown	Egypt		36992	ETISALAT-MISREG	false
197.237.113.182	unknown	Kenya		15399	WANANCHI-KE	false
197.166.142.82	unknown	Egypt		24863	LINKdotNET-ASEG	false
200.247.239.150	unknown	Brazil		4230	CLAROSABR	false
27.104.108.185	unknown	Singapore		4773	MOBILEONELTD-AS-APMobileOneLtdMobileInternetServicePr	false
197.172.142.211	unknown	South Africa		37168	CELL-CZA	false
38.21.161.24	unknown	United States		11738	BLIP-NETWORKSUS	false
41.122.114.233	unknown	South Africa		16637	MTNNS-ASZA	false
197.116.147.49	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.214.230.5	unknown	Morocco		36925	ASMediMA	false
197.60.6.64	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.251.253.116	unknown	Morocco		36903	MT-MPLSMA	false
155.226.30.158	unknown	United States		8698	NationwideBuildingSocietyGB	false
173.91.159.60	unknown	United States		10796	TWC-10796-MIDWESTUS	false
197.17.114.182	unknown	Tunisia		37693	TUNISIANATN	false
140.216.201.207	unknown	United States		22284	AS22284-DOI-OPSUS	false
45.227.105.139	unknown	Brazil		267019	AHPROVEDORTELECOMBR	false
197.213.165.228	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
197.149.160.154	unknown	South Africa		37438	GijimaZA	false
93.160.27.78	unknown	Denmark		3292	TDCTDCASDK	false
167.227.226.7	unknown	Canada		2675	CDAGOVNCA	false
38.14.196.18	unknown	United States		174	COGENT-174US	false
41.187.159.138	unknown	Egypt		20928	NOOR-ASEG	false
41.129.114.58	unknown	Egypt		24863	LINKdotNET-ASEG	false
36.97.133.30	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
41.76.191.241	unknown	Kenya		37225	NETWIDEZA	false
140.59.197.89	unknown	United States		668	DNIC-AS-00668US	false
197.102.233.98	unknown	South Africa		3741	ISZA	false
75.32.71.176	unknown	United States		7018	ATT-INTERNET4US	false
196.206.229.112	unknown	Morocco		36903	MT-MPLSMA	false
128.113.78.27	unknown	United States		91	RPI-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.74.76.29	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
156.124.100.151	unknown	United States		393504	XNSTGCA	false
5.232.36.131	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
156.111.212.186	unknown	United States		395139	NYP-INTERNETUS	false
156.2.12.217	unknown	United States		29975	VODACOM-ZA	false
198.193.143.103	unknown	United States		292	ESNET-WESTUS	false
197.60.132.79	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.240.45.199	unknown	unknown		37705	TOPNETTN	false
41.102.136.72	unknown	Algeria		36947	ALGTEL-ASDZ	false
138.146.210.40	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
45.93.168.231	unknown	Iran (ISLAMIC Republic Of)		57497	FARASOSAMANEHPASARGADIR	false
156.162.60.202	unknown	Egypt		36992	ETISALAT-MISREG	false
197.109.134.76	unknown	South Africa		37168	CELL-CZA	false
197.166.142.62	unknown	Egypt		24863	LINKdotNET-ASEG	false
41.129.114.69	unknown	Egypt		24863	LINKdotNET-ASEG	false
184.84.103.68	unknown	United States		9498	BBIL-APBHARTIAirtelLtdIN	false
41.116.238.207	unknown	South Africa		16637	MTNNS-ASZA	false
132.211.159.50	unknown	Canada		376	RISQ-ASCA	false
116.173.158.98	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
124.30.220.249	unknown	India		9583	SIFY-AS-INSifyLimitedIN	false
41.45.223.104	unknown	Egypt		8452	TE-ASTE-ASEG	false
75.140.122.137	unknown	United States		20115	CHARTER-20115US	false
156.254.22.239	unknown	Seychelles		394281	XHOSTSERVERUS	false
173.134.171.246	unknown	United States		10507	SPCSUS	false
197.233.228.76	unknown	Namibia		36999	TELECOM-NAMIBIANA	false
24.55.145.209	unknown	United States		3737	AS-PTDUS	false
9.78.182.57	unknown	United States		3356	LEVEL3US	false
158.214.11.66	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
156.145.214.10	unknown	United States		395139	NYP-INTERNETUS	false
108.195.224.187	unknown	United States		7018	ATT-INTERNET4US	false
197.177.27.84	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.121.74.189	unknown	Egypt		36992	ETISALAT-MISREG	false
177.235.47.208	unknown	Brazil		28573	CLAROSABR	false
167.217.255.66	unknown	United States		6461	ZAYO-6461US	false
53.4.254.107	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
190.132.225.189	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
94.35.200.63	unknown	Italy		8612	TISCALI-IT	false
197.250.1.124	unknown	Tanzania United Republic of		36908	VTL-ASNTZ	false
41.172.44.196	unknown	South Africa		36937	Neotel-ASZA	false
131.200.65.107	unknown	United States		14348	URI-ASUS	false
185.239.188.96	unknown	United Kingdom		205842	LINKWEBSOLUTIONSGB	false
177.129.86.241	unknown	Brazil		262393	AALVESGOMESINFORMATICA-MEBR	false
208.174.110.105	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
106.141.201.52	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
197.43.51.188	unknown	Egypt		8452	TE-ASTE-ASEG	false
159.42.98.107	unknown	United States		25019	SAUDINETSTC-ASSA	false
41.122.162.197	unknown	South Africa		16637	MTNNS-ASZA	false
124.50.156.109	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
81.172.40.105	unknown	Spain		12430	VODAFONE_ESES	false
64.4.89.121	unknown	Canada		7122	MTS-ASNCA	false
200.94.201.186	unknown	Mexico		6503	AxtelSABdeCVMX	false
36.219.124.155	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
129.7.152.93	unknown	United States		7276	UNIVERSITY-OF-HOUSTONUS	false
180.31.13.118	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
156.76.237.26	unknown	United States		6341	WIECUS	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
41.214.230.5	EXWofBp7D3	Get hash	malicious	Browse	
197.213.165.228	1u1hBVyy1i	Get hash	malicious	Browse	
156.66.10.209	arm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.132
	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	Filecoder.Hive_linux.bin	Get hash	malicious	Browse	• 162.213.33.108
	yFbmGHoONE	Get hash	malicious	Browse	• 162.213.33.108
	zju8TB277l	Get hash	malicious	Browse	• 162.213.33.108
	JYWlIP5wHP	Get hash	malicious	Browse	• 162.213.33.108
	uwgXkY20gB	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.132
	FWsCarsq8Q	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	arm	Get hash	malicious	Browse	• 162.213.33.132

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UUNETUS	x86	Get hash	malicious	Browse	• 72.79.77.130
	arm	Get hash	malicious	Browse	• 108.31.113.0
	H7MTKzOUnc	Get hash	malicious	Browse	• 71.121.91.170
	gL6zNW1uNj	Get hash	malicious	Browse	• 100.49.35.79
	mF0Mqdkjfz	Get hash	malicious	Browse	• 108.31.254.148
	sora.arm7	Get hash	malicious	Browse	• 204.148.94.234
	z0x3n.arm7-20211110-2150	Get hash	malicious	Browse	• 65.241.94.126
	z0x3n.arm-20211110-2150	Get hash	malicious	Browse	• 207.77.250.122
	sora.mpsl	Get hash	malicious	Browse	• 108.17.85.21
	sora.arm5	Get hash	malicious	Browse	• 71.251.160.125
	l0vNaPgd6f	Get hash	malicious	Browse	• 65.239.141.150
	8fVDxGRR8S	Get hash	malicious	Browse	• 68.133.123.68
	s36oh8l6l0	Get hash	malicious	Browse	• 212.209.129.233
	63BjZ1IcIh	Get hash	malicious	Browse	• 71.183.144.186
	trynagetmybinsufucker98575.arm7	Get hash	malicious	Browse	• 96.243.103.196
	QXFOZ3Cshc	Get hash	malicious	Browse	• 100.4.94.85
	sora.x86	Get hash	malicious	Browse	• 63.104.43.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sora.arm7	Get hash	malicious	Browse	• 71.182.1.251
	sora.arm	Get hash	malicious	Browse	• 173.49.194.4
	lDawzTbABc	Get hash	malicious	Browse	• 71.242.116.79
CISGCentrumInformacjiSpoleczno-GospodarczejPL	Qm6vTXPjLh	Get hash	malicious	Browse	• 158.66.187.78
	pandora.arm	Get hash	malicious	Browse	• 158.66.83.98
	hoho.arm7	Get hash	malicious	Browse	• 158.66.163.88
	zCS6X4TGYb	Get hash	malicious	Browse	• 158.66.163.73
	k511cDa8ud	Get hash	malicious	Browse	• 158.66.199.40
	fL3XyDrYfF	Get hash	malicious	Browse	• 158.66.151.87
	LDWhPg4vRM	Get hash	malicious	Browse	• 158.66.240.172
IAM-ASMA	x86	Get hash	malicious	Browse	• 197.131.5.169
	gL6zNW1uNj	Get hash	malicious	Browse	• 102.55.170.247
	sora.mips	Get hash	malicious	Browse	• 197.130.113.61
	s36oh8l6l0	Get hash	malicious	Browse	• 105.141.114.186
	X5bKvoLX1E	Get hash	malicious	Browse	• 196.94.241.27
	hz4vFpTJb8	Get hash	malicious	Browse	• 160.168.12.251
	Yoshi.arm7-20211110-0350	Get hash	malicious	Browse	• 160.163.34.124
	2tdWqgPQPc	Get hash	malicious	Browse	• 197.130.137.72
	v9o2vinbUj	Get hash	malicious	Browse	• 105.132.245.149
	SQFoFeC1jQ	Get hash	malicious	Browse	• 197.130.162.16
	byxEpar5Zm	Get hash	malicious	Browse	• 197.128.32.85
	tDfXtXb4Oz	Get hash	malicious	Browse	• 160.162.216.193
	y2NMF6ulOI	Get hash	malicious	Browse	• 196.94.216.88
	8krBRiWrtG	Get hash	malicious	Browse	• 193.194.39.45
	673ArEEjFZ	Get hash	malicious	Browse	• 193.194.39.41
	AER0hx5txK	Get hash	malicious	Browse	• 105.153.80.179
	bZ3EzTJKiD	Get hash	malicious	Browse	• 154.151.203.26
	rMwxCtXmuJ	Get hash	malicious	Browse	• 154.148.133.158
	WsoVopfjnC	Get hash	malicious	Browse	• 102.73.178.212
	sora.x86	Get hash	malicious	Browse	• 160.165.145.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink

Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.9219280948873623
Encrypted:	false
SSDEEP:	3:5bkPn:pkP
MD5:	FF001A15CE15CF062A3704CEA2991B5F
SHA1:	B06F6855F376C3245B82212AC73ADED55DFE5DEF
SHA-256:	C54830B41ECFA1B6FBDC30397188DDA86B7B200E62AEAC21AE694A6192DCC38A
SHA-512:	65EBF7C31F6F65713CE01B38A112E97D0AE64A6BD1DA40CE4C1B998F10CD3912EE1A48BB2B279B24493062118AAB3B8753742E2AF28E56A31A7AAB27DE80E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.

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

/proc/5365/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):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:DTQv:P6
MD5:	722854F46BE7C55F62C4033DA6ADE94B
SHA1:	F74E66117C97C8CE0F8EEC94B7E2B92A9D38337F
SHA-256:	E832BBB35129DD49811FBF5BA32A3611AC68E39C41F213A459E275ABBF1F5941
SHA-512:	59CF8449A3AFF33E013E446F294A3C77EC973552A3C55C6B5C048EF7E62EEE5E4C3F08554E33D4016F6674389357393BB2568397D09FC067E557EF8D61D2251F
Malicious:	false
Reputation:	low
Preview:	5365.

/run/systemd/resolve/stub-resolv.conf	
Process:	/tmp/arm7
File Type:	ASCII text
Category:	dropped
Size (bytes):	38
Entropy (8bit):	3.3918926446809334
Encrypted:	false
SSDEEP:	3:KkZRAkd:KaAu
MD5:	C7EA09D26E26605227076E0514A33038
SHA1:	C3F9736E9AF7BD0885578859A50B205C8FA5FC8E
SHA-256:	7E8AD76E0D200E93918CA2E93C99FF8ECD02071953BF1479819DB3AC0DBB6D07
SHA-512:	17D0088725EB9991E9EB82E8A3DE0878E45E6F394BBC2AD260AA59C786FF0AD565E145E21256425D1C0ABE15F3ECB402EBB0A6A5E1C2D5BA7A4D95EC93A2861F
Malicious:	false

/run/systemd/resolve/stub-resolv.conf	
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):	2.321928094887362
Encrypted:	false
SSDEEP:	3:E8v:E+
MD5:	CE7838A8404B6917B0897DCE5B6C7095
SHA1:	AB43E603CAF13ABBBCD8EC9793F4ACE12EB09F0B
SHA-256:	1828BE2C5CDA4C0CFE7F0F8ABC2AE26E377E9D0CC02937E18CADAF866F30994A
SHA-512:	F0C4216DCC182947DC9765A97DFC8C1454A8C6C03D8D6E815C0F64ACD390131F4AB1CB722DA134887A259FA78B917CE4C85AC54537573CAA45017DCDF145F46
Malicious:	false
Reputation:	low
Preview:	5403.

/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:	57D0856EC65558B4A843A4696B644AC3E80B3EA0E6EC1C2FAC7A00015B96EBB2CC30967EB8DEFC3E648E59AC6882F6A4F69468D4B6CD0FD60F9F343C206DBFBC
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 nouveau 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? yes.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:FSen:Z
MD5:	E43A10DB72BACE9741B8591C226777AE
SHA1:	3A02096DA23FDF8B108D6F96E6F73B38DE0654A6
SHA-256:	49F4D88EF58629CFA6F9CB3F4732FDF8DA06E81FC81CDD3F7CAD8ABA69DC6C80
SHA-512:	392400F7CC2B6282BE6691FE137FE96524540D811A76A61E85F7FB36CB175D22F9D2E282AAFA97884CD8F95E79A0ED5AC36A3368D57DF03C97FBACEA6917FDE0
Malicious:	false
Preview:	5579.

Static File Info

General	
File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.988872339172871
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm7
File size:	77060
MD5:	9fc0975479e319f970c96eded3c2d001
SHA1:	ff77399d8fb757636a3eae4909dbc33f4a00f09e
SHA256:	f0c7eb51c588fa50e39bee022ea2c4f602842012b01f2ee025b91eb5eb50782f
SHA512:	76e5429bd9c9501324084d504173e79354d8f24dc1852c02d8d0d2d4fab7468b133488a88f9ad3cb74d02c5aa7784dfe1165469bdfc1acd38bc723c908dc6164
SSDEEP:	1536:TT9/c4ITNRcVbXye47li0XD3tbBm3wvkte38LRdeU98ZMrk1LVon2dt9:VkeBXv4Bi0XD3xs3wsk8L7jjY7q2x
File Content Preview:	.ELF.....(.....8S..4.....4. ...(.....%...%.....p'..p...p.....Q.td.....?..`UPX !.....2...2.....k.....?.E.h;....#..$...o...m.W.I...ef?....$m.:I....j..8....+}.?..`.j.oB.!.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x15338
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0xe525	0xe525	4.0200	0x5	R E	0x8000		
LOAD	0x2770	0x3a770	0x3a770	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 11, 2021 03:08:56.256854057 CET	192.168.2.23	8.8.8.8	0x553f	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Nov 11, 2021 03:08:56.256911039 CET	192.168.2.23	8.8.8.8	0xd530	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 11, 2021 03:08:56.273183107 CET	8.8.8.8	192.168.2.23	0x553f	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Nov 11, 2021 03:08:56.273183107 CET	8.8.8.8	192.168.2.23	0x553f	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: arm7 PID: 5234 Parent PID: 5112

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	/tmp/arm7
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: arm7 PID: 5236 Parent PID: 5234

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5237 Parent PID: 5234

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5239 Parent PID: 5234

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7

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

Analysis Process: arm7 PID: 5240 Parent PID: 5234

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5241 Parent PID: 5234

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5245 Parent PID: 5234

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5249 Parent PID: 5245

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5251 Parent PID: 5245

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: 5253 Parent PID: 5251

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Written

Analysis Process: arm7 PID: 5255 Parent PID: 5253

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5255 Parent PID: 5253

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/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: 5257 Parent PID: 5255

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5257 Parent PID: 5255

General

Start time:	03:08:09
Start date:	11/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/arm7 /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /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: arm7 PID: 5262 Parent PID: 5253

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5262 Parent PID: 5253

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "rm -rf /var/log/wtmp"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5268 Parent PID: 5262

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5268 Parent PID: 5262

General

Start time:	03:08:20
Start date:	11/11/2021
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: arm7 PID: 5269 Parent PID: 5253

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5269 Parent PID: 5253

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "rm -rf /tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5271 Parent PID: 5269

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5271 Parent PID: 5269

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/*
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: arm7 PID: 5272 Parent PID: 5253

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5272 Parent PID: 5253

General

Start time:	03:08:20
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "rm -rf /bin/netstat"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5274 Parent PID: 5272

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5274 Parent PID: 5272

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /bin/netstat
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: arm7 PID: 5275 Parent PID: 5253

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5275 Parent PID: 5253

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -F"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5277 Parent PID: 5275

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5277 Parent PID: 5275

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/usr/sbin/iptables
Arguments:	iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: arm7 PID: 5281 Parent PID: 5253

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5281 Parent PID: 5253

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "pkill -9 busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5284 Parent PID: 5281

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5284 Parent PID: 5281

General

Start time:	03:08:21
Start date:	11/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 busybox
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5287 Parent PID: 5253

General

Start time:	03:08:23
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5287 Parent PID: 5253

General

Start time:	03:08:23
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "pkill -9 perl"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5289 Parent PID: 5287

General

Start time:	03:08:23
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5289 Parent PID: 5287

General

Start time:	03:08:23
Start date:	11/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 perl
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5292 Parent PID: 5253

General

Start time:	03:08:25
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5292 Parent PID: 5253

General

Start time:	03:08:25
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "pkill -9 python"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5294 Parent PID: 5292

General

Start time:	03:08:25
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5294 Parent PID: 5292

General

Start time:	03:08:25
Start date:	11/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 python
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5295 Parent PID: 5253

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5295 Parent PID: 5253

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "service iptables stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5297 Parent PID: 5295

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5297 Parent PID: 5295

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	service iptables stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: 5299 Parent PID: 5297

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5299 Parent PID: 5297

General

Start time:	03:08:28

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

File Activities

File Read

Analysis Process: service PID: 5300 Parent PID: 5297

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5300 Parent PID: 5297

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5301 Parent PID: 5297

General

Start time:	03:08:28
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5301 Parent PID: 5297

General

Start time:	03:08:28
Start date:	11/11/2021
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: 5302 Parent PID: 5297

General

Start time:	03:08:29
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5303 Parent PID: 5302

General

Start time:	03:08:29
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5303 Parent PID: 5302

General

Start time:	03:08:29
Start date:	11/11/2021
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: 5304 Parent PID: 5302

General

Start time:	03:08:29
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5304 Parent PID: 5302

General

Start time:	03:08:29
Start date:	11/11/2021
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: 5297 Parent PID: 5295

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl stop iptables.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: arm7 PID: 5308 Parent PID: 5253

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5308 Parent PID: 5253

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "/sbin/iptables -F; /sbin/iptables -X"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5310 Parent PID: 5308

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5310 Parent PID: 5308

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/sbin/iptables
Arguments:	/sbin/iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: sh PID: 5311 Parent PID: 5308

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5311 Parent PID: 5308

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/sbin/iptables
Arguments:	/sbin/iptables -X
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: arm7 PID: 5312 Parent PID: 5253

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5312 Parent PID: 5253

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "service firewalld stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5314 Parent PID: 5312

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5314 Parent PID: 5312

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	service firewalld stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: 5315 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5315 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5316 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5316 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5317 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5317 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
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: 5318 Parent PID: 5314

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5319 Parent PID: 5318

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5319 Parent PID: 5318

General

Start time:	03:08:32
Start date:	11/11/2021
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: 5320 Parent PID: 5318

General

Start time:	03:08:32
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5320 Parent PID: 5318

General

Start time:	03:08:32
Start date:	11/11/2021
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: 5314 Parent PID: 5312

General

Start time:	03:08:36
Start date:	11/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl stop firewalld.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: arm7 PID: 5323 Parent PID: 5253

General

Start time:	03:08:36

Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5323 Parent PID: 5253

General

Start time:	03:08:36
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "rm -rf ~/.bash_history"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5325 Parent PID: 5323

General

Start time:	03:08:36
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5325 Parent PID: 5323

General

Start time:	03:08:36
Start date:	11/11/2021
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: arm7 PID: 5326 Parent PID: 5253

General

Start time:	03:08:36

Start date:	11/11/2021
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5326 Parent PID: 5253

General

Start time:	03:08:36
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "history -c"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5355 Parent PID: 1

General

Start time:	03:08:55
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5355 Parent PID: 1

General

Start time:	03:08:55
Start date:	11/11/2021
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: 5364 Parent PID: 1

General

Start time:	03:08:59
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5364 Parent PID: 1

General

Start time:	03:08:59
Start date:	11/11/2021
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: 5365 Parent PID: 1

General

Start time:	03:08:59
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5365 Parent PID: 1

General

Start time:	03:08:59
Start date:	11/11/2021
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: 5370 Parent PID: 1320

General

Start time:	03:09:06
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5370 Parent PID: 1320

General

Start time:	03:09:06
Start date:	11/11/2021
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: 5373 Parent PID: 1320

General

Start time:	03:09:06
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5373 Parent PID: 1320

General

Start time:	03:09:06
Start date:	11/11/2021
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: 5374 Parent PID: 1

General

Start time:	03:09:06
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5374 Parent PID: 1

General

Start time:	03:09:06
Start date:	11/11/2021
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: 5403 Parent PID: 1860

General

Start time:	03:09:28
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5403 Parent PID: 1860

General

Start time:	03:09:28
Start date:	11/11/2021
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: 5428 Parent PID: 1

General

Start time:	03:09:32
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5428 Parent PID: 1

General

Start time:	03:09:32
Start date:	11/11/2021
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: 5429 Parent PID: 5428

General

Start time:	03:09:32
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5429 Parent PID: 5428

General

Start time:	03:09:32
Start date:	11/11/2021
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: 5430 Parent PID: 5429

General

Start time:	03:09:32
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5430 Parent PID: 5429

General

Start time:	03:09:32
Start date:	11/11/2021
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: 5431 Parent PID: 5428

General

Start time:	03:09:32
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5431 Parent PID: 5428

General

Start time:	03:09:32
Start date:	11/11/2021
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: 5432 Parent PID: 5431

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5432 Parent PID: 5431

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5433 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5433 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021

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: 5434 Parent PID: 5433

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5434 Parent PID: 5433

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5435 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5435 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5436 Parent PID: 5435

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5436 Parent PID: 5435

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5437 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5437 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5438 Parent PID: 5437

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5438 Parent PID: 5437

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5439 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5439 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5440 Parent PID: 5439

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5440 Parent PID: 5439

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5441 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5441 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5442 Parent PID: 5441

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5442 Parent PID: 5441

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5443 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5443 Parent PID: 5428

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5444 Parent PID: 5443

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5444 Parent PID: 5443

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5445 Parent PID: 1

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5445 Parent PID: 1

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5446 Parent PID: 5445

General

Start time:	03:09:33
Start date:	11/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5446 Parent PID: 5445

General

Start time:	03:09:33
Start date:	11/11/2021
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: 5452 Parent PID: 1

General

Start time:	03:09:35
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5452 Parent PID: 1

General

Start time:	03:09:35
Start date:	11/11/2021
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: 5456 Parent PID: 2038

General

Start time:	03:09:41
Start date:	11/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5456 Parent PID: 2038

General

Start time:	03:09:41
Start date:	11/11/2021
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: 5476 Parent PID: 1

General

Start time:	03:09:44
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5476 Parent PID: 1

General

Start time:	03:09:44
Start date:	11/11/2021
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: 5500 Parent PID: 1

General

Start time:	03:09:45
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5500 Parent PID: 1

General

Start time:	03:09:45
Start date:	11/11/2021
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: 5550 Parent PID: 1

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5550 Parent PID: 1

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5551 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5551 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5552 Parent PID: 5551

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5552 Parent PID: 5551

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5553 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5553 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5554 Parent PID: 5553

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5554 Parent PID: 5553

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5555 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5555 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5556 Parent PID: 5555

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5556 Parent PID: 5555

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5557 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5557 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5558 Parent PID: 5557

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5558 Parent PID: 5557

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5559 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5559 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5560 Parent PID: 5559

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5560 Parent PID: 5559

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5561 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5561 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021

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: 5562 Parent PID: 5561

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5562 Parent PID: 5561

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5563 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5563 Parent PID: 5550

General

Start time:	03:11:17

Start date:	11/11/2021
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: 5564 Parent PID: 5563

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5564 Parent PID: 5563

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5565 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5565 Parent PID: 5550

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5566 Parent PID: 5565

General

Start time:	03:11:17
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5566 Parent PID: 5565

General

Start time:	03:11:17
Start date:	11/11/2021
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: 5567 Parent PID: 1

General

Start time:	03:11:18
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5567 Parent PID: 1

General

Start time:	03:11:18
Start date:	11/11/2021
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: 5568 Parent PID: 5567

General

Start time:	03:11:18
Start date:	11/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5568 Parent PID: 5567

General

Start time:	03:11:18
Start date:	11/11/2021
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: 5569 Parent PID: 1

General

Start time:	03:11:20
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5569 Parent PID: 1

General

Start time:	03:11:20
Start date:	11/11/2021
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: 5579 Parent PID: 1

General

Start time:	03:11:30
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5579 Parent PID: 1

General

Start time:	03:11:30
Start date:	11/11/2021
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