ID: 519694
Sample Name: x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:02:50
Date: 11/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

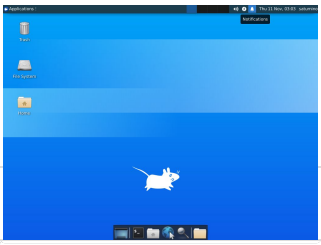
Linux Analysis Report x86

Overview

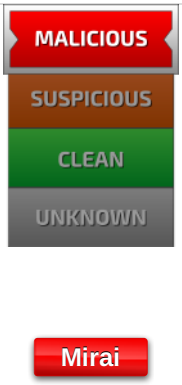
General Information

Sample Name:	x86
Analysis ID:	519694
MD5:	776097f22f49b5f…
SHA1:	540cb7d95922f31.
SHA256:	c817429ed299ec..
Tags:	Mirai
Infos:	

Most interesting Screenshot:



Detection

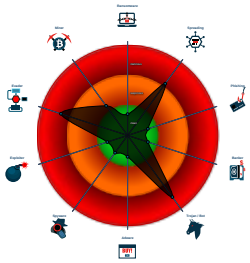


Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample tries to kill many processes…
- 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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	519694
Start date:	11.11.2021
Start time:	03:02:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	x86
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal96.spre.troj.evad.lin@0/9@2/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- x86 (PID: 5245, Parent: 5120, MD5: 776097f22f49b5f4c467e2afdee63009) Arguments: /tmp/x86
  - x86 New Fork (PID: 5246, Parent: 5245)
  - x86 New Fork (PID: 5247, Parent: 5245)
  - x86 New Fork (PID: 5249, Parent: 5245)
  - x86 New Fork (PID: 5250, Parent: 5245)
  - x86 New Fork (PID: 5251, Parent: 5245)
  - x86 New Fork (PID: 5252, Parent: 5245)
    - x86 New Fork (PID: 5253, Parent: 5252)
    - x86 New Fork (PID: 5254, Parent: 5252)
      - x86 New Fork (PID: 5255, Parent: 5254)

- x86 New Fork (PID: 5256, Parent: 5255)
  - sh (PID: 5256, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
    - sh New Fork (PID: 5257, Parent: 5256)
      - rm (PID: 5257, Parent: 5256, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /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-lofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /tmp/x86 /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
- x86 New Fork (PID: 5265, Parent: 5255)
  - sh (PID: 5265, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /var/log/wtmp"
    - sh New Fork (PID: 5266, Parent: 5265)
      - rm (PID: 5266, Parent: 5265, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
- x86 New Fork (PID: 5267, Parent: 5255)
  - sh (PID: 5267, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/*"
    - sh New Fork (PID: 5268, Parent: 5267)
      - rm (PID: 5268, Parent: 5267, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
- x86 New Fork (PID: 5269, Parent: 5255)
  - sh (PID: 5269, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /bin/netstat"
    - sh New Fork (PID: 5270, Parent: 5269)
      - rm (PID: 5270, Parent: 5269, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
- x86 New Fork (PID: 5271, Parent: 5255)
  - sh (PID: 5271, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -F"
    - sh New Fork (PID: 5272, Parent: 5271)
      - iptables (PID: 5272, Parent: 5271, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -F
- x86 New Fork (PID: 5276, Parent: 5255)
  - sh (PID: 5276, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 busybox"
    - sh New Fork (PID: 5278, Parent: 5276)
      - pkill (PID: 5278, Parent: 5276, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
- x86 New Fork (PID: 5283, Parent: 5255)
  - sh (PID: 5283, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 perl"
    - sh New Fork (PID: 5284, Parent: 5283)
      - pkill (PID: 5284, Parent: 5283, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
- x86 New Fork (PID: 5285, Parent: 5255)
  - sh (PID: 5285, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 python"
    - sh New Fork (PID: 5286, Parent: 5285)
      - pkill (PID: 5286, Parent: 5285, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
- x86 New Fork (PID: 5289, Parent: 5255)
  - sh (PID: 5289, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service iptables stop"
    - sh New Fork (PID: 5290, Parent: 5289)
      - service (PID: 5290, Parent: 5289, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service iptables stop
        - service New Fork (PID: 5292, Parent: 5290)
          - basename (PID: 5292, Parent: 5290, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5293, Parent: 5290)
          - basename (PID: 5293, Parent: 5290, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5294, Parent: 5290)
          - systemctl (PID: 5294, Parent: 5290, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
        - service New Fork (PID: 5295, Parent: 5290)
          - service New Fork (PID: 5296, Parent: 5295)
            - systemctl (PID: 5296, Parent: 5295, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
          - service New Fork (PID: 5297, Parent: 5295)
            - sed (PID: 5297, Parent: 5295, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
      - systemctl (PID: 5290, Parent: 5289, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop iptables.service
- x86 New Fork (PID: 5300, Parent: 5255)
  - sh (PID: 5300, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "/sbin/iptables -F; /sbin/iptables -X"
    - sh New Fork (PID: 5301, Parent: 5300)
      - iptables (PID: 5301, Parent: 5300, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -F
    - sh New Fork (PID: 5302, Parent: 5300)
      - iptables (PID: 5302, Parent: 5300, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -X
- x86 New Fork (PID: 5303, Parent: 5255)
  - sh (PID: 5303, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service firewalld stop"
    - sh New Fork (PID: 5304, Parent: 5303)
      - service (PID: 5304, Parent: 5303, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service firewalld stop
        - service New Fork (PID: 5305, Parent: 5304)
          - basename (PID: 5305, Parent: 5304, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5306, Parent: 5304)
          - basename (PID: 5306, Parent: 5304, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
        - service New Fork (PID: 5307, Parent: 5304)
          - systemctl (PID: 5307, Parent: 5304, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
        - service New Fork (PID: 5308, Parent: 5304)
          - service New Fork (PID: 5309, Parent: 5308)
            - systemctl (PID: 5309, Parent: 5308, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
          - service New Fork (PID: 5310, Parent: 5308)
            - sed (PID: 5310, Parent: 5308, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
      - systemctl (PID: 5304, Parent: 5303, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop firewalld.service
- x86 New Fork (PID: 5311, Parent: 5255)
  - sh (PID: 5311, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf ~/.bash_history"
    - sh New Fork (PID: 5312, Parent: 5311)
      - rm (PID: 5312, Parent: 5311, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /root/.bash_history

- x86 New Fork (PID: 5313, Parent: 5255)
- sh (PID: 5313, Parent: 5255, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "history -c"

- systemd New Fork (PID: 5337, Parent: 1)
- whoopsie (PID: 5337, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5367, Parent: 1)
- sshd (PID: 5367, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5368, Parent: 1)
- sshd (PID: 5368, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5371, Parent: 1320)
- Default (PID: 5371, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5372, Parent: 1320)
- Default (PID: 5372, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5375, Parent: 1)
- accounts-daemon (PID: 5375, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
- systemd New Fork (PID: 5410, Parent: 1860)
- pulseaudio (PID: 5410, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5435, Parent: 1)
- gpu-manager (PID: 5435, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5436, Parent: 5435)
  - sh (PID: 5436, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5437, Parent: 5436)
    - grep (PID: 5437, Parent: 5436, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5438, Parent: 5435)
  - sh (PID: 5438, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5439, Parent: 5438)
    - grep (PID: 5439, Parent: 5438, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5440, Parent: 5435)
  - sh (PID: 5440, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5441, Parent: 5440)
    - grep (PID: 5441, Parent: 5440, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5442, Parent: 5435)
  - sh (PID: 5442, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5443, Parent: 5442)
    - grep (PID: 5443, Parent: 5442, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5444, Parent: 5435)
  - sh (PID: 5444, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5445, Parent: 5444)
    - grep (PID: 5445, Parent: 5444, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5446, Parent: 5435)
  - sh (PID: 5446, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5447, Parent: 5446)
    - grep (PID: 5447, Parent: 5446, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5451, Parent: 5435)
  - sh (PID: 5451, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5452, Parent: 5451)
    - grep (PID: 5452, Parent: 5451, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5453, Parent: 5435)
  - sh (PID: 5453, Parent: 5435, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5454, Parent: 5453)
    - grep (PID: 5454, Parent: 5453, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5455, Parent: 1)
- generate-config (PID: 5455, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5456, Parent: 5455)
  - pkill (PID: 5456, Parent: 5455, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5457, Parent: 1)
- gdm-wait-for-drm (PID: 5457, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- gvfsd-fuse New Fork (PID: 5462, Parent: 2038)
- fusermount (PID: 5462, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5475, Parent: 1)
- systemd-user-runtime-dir (PID: 5475, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5502, Parent: 1)
- gdm3 (PID: 5502, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- systemd New Fork (PID: 5553, Parent: 1)
- gpu-manager (PID: 5553, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
  - gpu-manager New Fork (PID: 5554, Parent: 5553)
  - sh (PID: 5554, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
    - sh New Fork (PID: 5555, Parent: 5554)
    - grep (PID: 5555, Parent: 5554, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5556, Parent: 5553)
  - sh (PID: 5556, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
    - sh New Fork (PID: 5557, Parent: 5556)

- grep (PID: 5557, Parent: 5556, 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: 5558, Parent: 5553)
- sh (PID: 5558, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5559, Parent: 5558)
  - grep (PID: 5559, Parent: 5558, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5560, Parent: 5553)
- sh (PID: 5560, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5561, Parent: 5560)
  - grep (PID: 5561, Parent: 5560, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5562, Parent: 5553)
- sh (PID: 5562, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5563, Parent: 5562)
  - grep (PID: 5563, Parent: 5562, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5564, Parent: 5553)
- sh (PID: 5564, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5565, Parent: 5564)
  - grep (PID: 5565, Parent: 5564, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5566, Parent: 5553)
- sh (PID: 5566, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5567, Parent: 5566)
  - grep (PID: 5567, Parent: 5566, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5568, Parent: 5553)
- sh (PID: 5568, Parent: 5553, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5569, Parent: 5568)
  - grep (PID: 5569, Parent: 5568, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5570, Parent: 1)
- generate-config (PID: 5570, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5571, Parent: 5570)
  - pkill (PID: 5571, Parent: 5570, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5574, Parent: 1)
- gdm-wait-for-drm (PID: 5574, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5582, Parent: 1)
- gdm3 (PID: 5582, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- **cleanup**

Yara Overview

Initial Sample

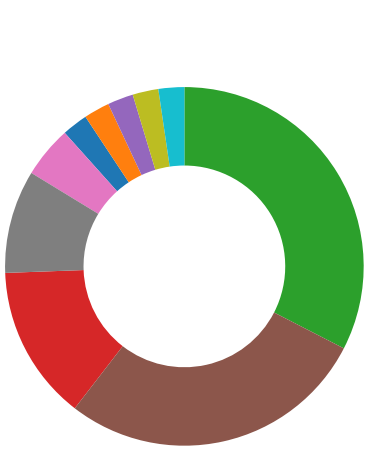
Source	Rule	Description	Author	Strings
x86	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xa10d:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xa0b9:$s2: $Id: UPX • 0xa06a:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Jbx Signature Overview

- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior



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:

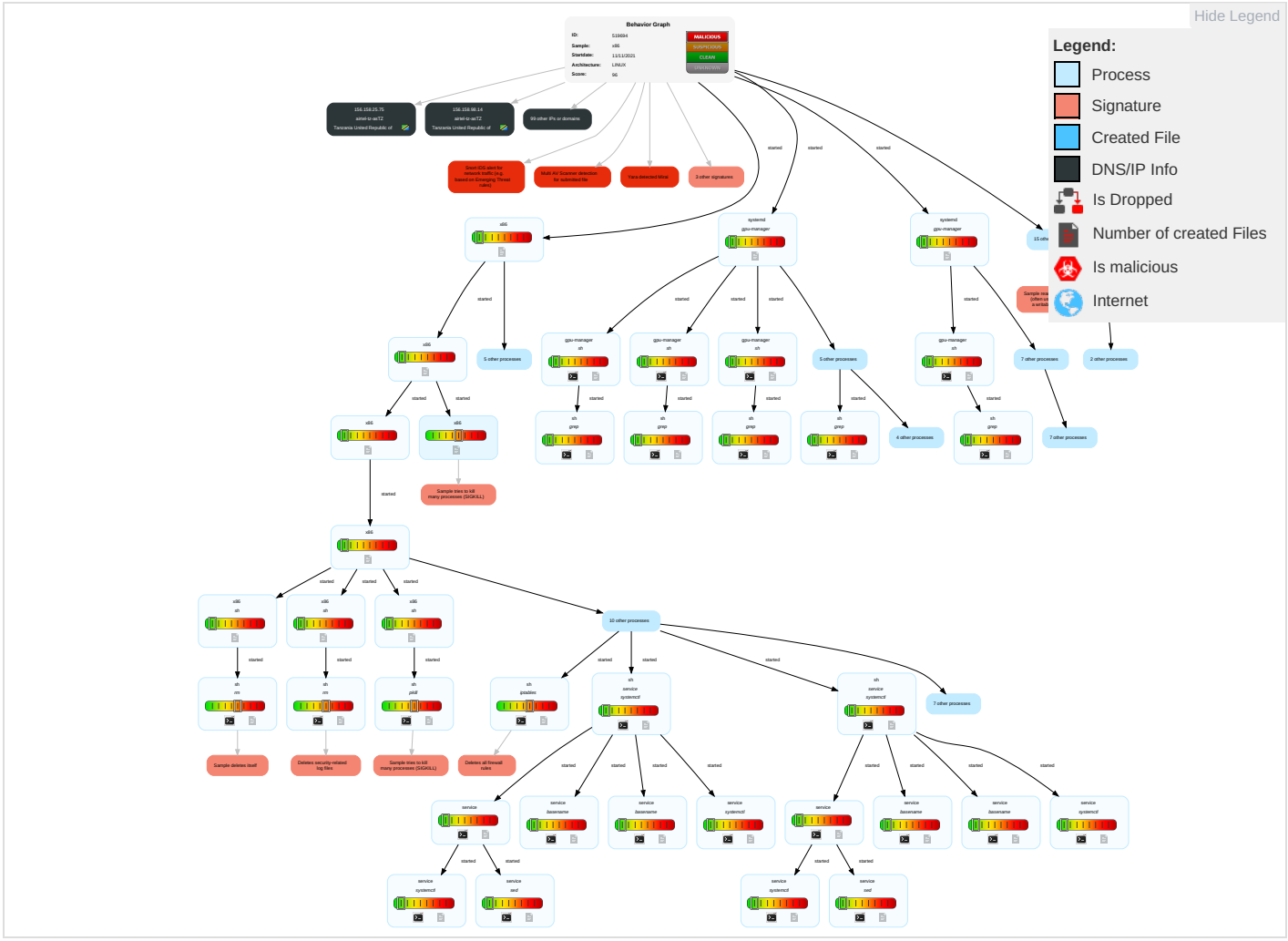
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
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	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
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	D L
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	D D
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		C E F
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		M A F F
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		A A F
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		D E f
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		C F A F

Malware Configuration

No configs have been found

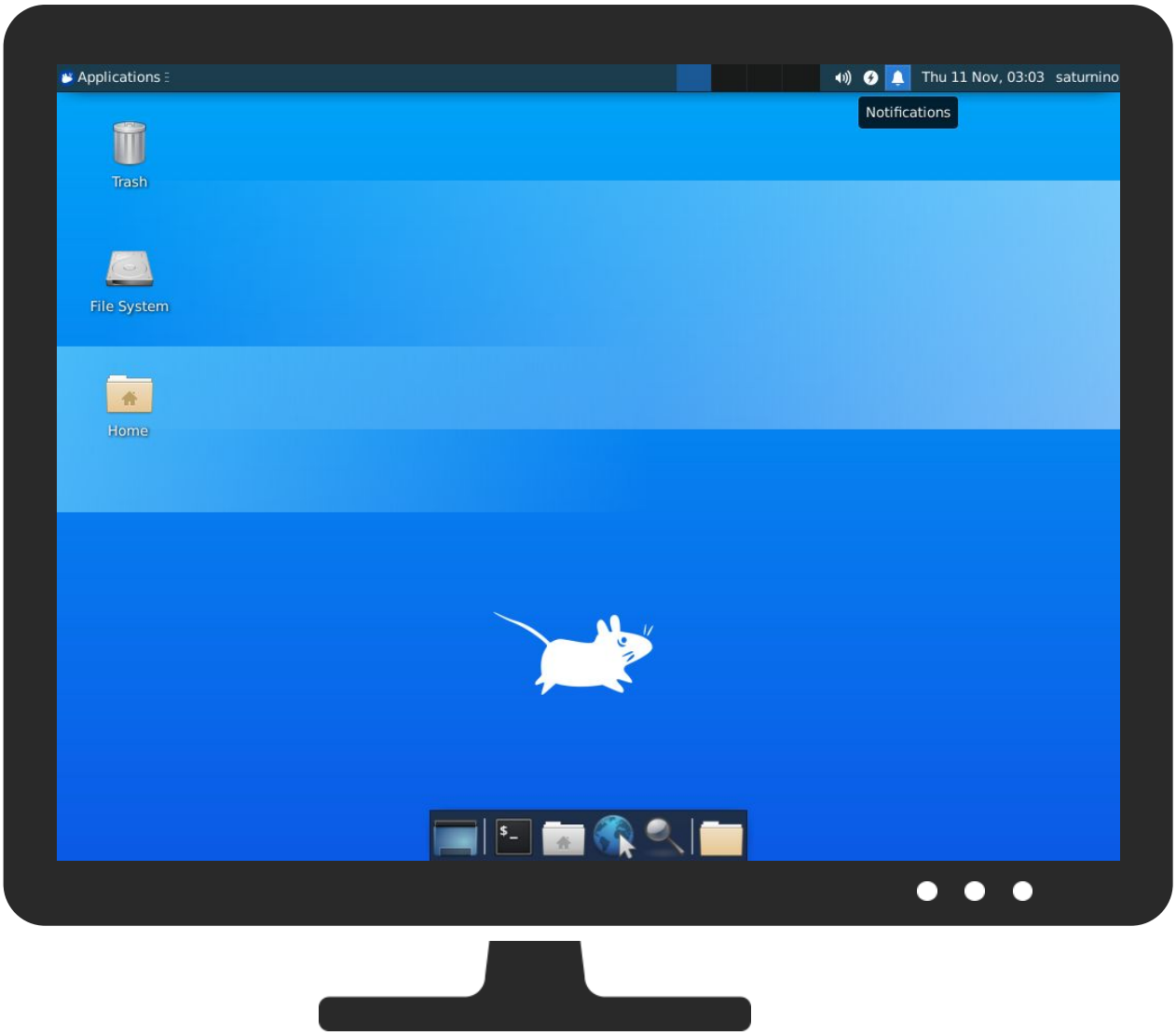
Behavior Graph



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
x86	35%	Virustotal		Browse
x86	34%	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
59.165.159.36	unknown	India		4755	TATACOMM-ASTATACommunicationsformerlyVSNLisLeadingISP	false
156.158.98.14	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
126.139.65.215	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
41.102.150.109	unknown	Algeria		36947	ALGTEL-ASDZ	false
145.30.21.7	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
197.116.172.19	unknown	Algeria		36947	ALGTEL-ASDZ	false
32.81.194.163	unknown	United States		2686	ATGS-MMD-ASUS	false
67.241.131.148	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
41.57.232.57	unknown	Ghana		37103	BUSYINTERNETGH	false
156.246.150.168	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
156.134.83.77	unknown	United States		12217	UPSUS	false
155.167.205.84	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
156.48.59.142	unknown	United Kingdom		29975	VODACOM-ZA	false
197.153.12.90	unknown	Morocco		36925	ASMediMA	false
198.10.206.121	unknown	United States		24	AS24US	false
156.154.241.62	unknown	United States		19905	NEUSTAR-AS6US	false
96.205.253.26	unknown	United States		7922	COMCAST-7922US	false
216.47.150.26	unknown	United States		29825	IIT-NETWORK-ASUS	false
135.222.165.169	unknown	United States		10455	LUCENT-CIOUS	false
197.181.96.243	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
4.131.82.38	unknown	United States		3356	LEVEL3US	false
175.106.189.22	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
156.49.135.42	unknown	Sweden		29975	VODACOM-ZA	false
132.208.44.133	unknown	Canada		376	RISQ-ASCA	false
197.53.167.23	unknown	Egypt		8452	TE-ASTE-ASEG	false
201.138.200.133	unknown	Mexico		8151	UninetSAdeCVMX	false
41.198.255.152	unknown	South Africa		328306	Avanti-ASZA	false
185.188.72.147	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.42.142.158	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.235.45.185	unknown	Seychelles		134705	ITACE-AS-APItaceInternationalLimitedHK	false
80.31.124.83	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
221.160.166.162	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
178.157.234.78	unknown	Denmark		43557	ASEMNETDK	false
156.154.241.72	unknown	United States		19905	NEUSTAR-AS6US	false
156.22.182.88	unknown	Australia		29975	VODACOM-ZA	false
156.235.189.160	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
197.237.113.178	unknown	Kenya		15399	WANANCHI-KE	false
157.244.145.111	unknown	Canada		32934	FACEBOOKUS	false
156.72.230.178	unknown	United States		29975	VODACOM-ZA	false
197.130.137.73	unknown	Morocco		6713	IAM-ASMA	false
41.60.37.68	unknown	Mauritius		30969	ZOL-ASGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
60.25.152.140	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
72.79.77.130	unknown	United States		701	UUNETUS	false
197.114.121.159	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.143.173.219	unknown	Algeria		36891	ICOSNET-ASDZ	false
41.215.59.59	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUP LTDisanISPservingKE	false
119.189.161.217	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
48.202.227.50	unknown	United States		2686	ATGS-MMD-ASUS	false
41.199.209.17	unknown	Egypt		36992	ETISALAT-MISREG	false
83.223.101.1	unknown	United Kingdom		29017	GYRONGB	false
197.66.206.25	unknown	South Africa		16637	MTNNS-ASZA	false
156.197.151.2	unknown	Egypt		8452	TE-ASTE-ASEG	false
101.254.64.50	unknown	China		23724	CHINANET-IDC-BJ-APIDCChinaTelecommunicationsCorporation	false
156.197.234.78	unknown	Egypt		8452	TE-ASTE-ASEG	false
140.178.218.215	unknown	United States		668	DNIC-AS-00668US	false
156.147.203.94	unknown	Korea Republic of		4668	LGNET-AS-KRLGCNSKR	false
156.230.199.6	unknown	Seychelles		134705	ITACE-AS-APItaceInternationalLimitedHK	false
95.107.112.141	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
186.52.71.22	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
149.78.207.23	unknown	United States		46356	SBUEDUUS	false
94.55.185.136	unknown	Turkey		47524	TURKSAT-ASTR	false
158.99.140.160	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
197.237.248.156	unknown	Kenya		15399	WANANCHI-KE	false
91.84.192.4	unknown	United Kingdom		12513	ECLIPSEGB	false
205.133.146.227	unknown	United States		600	OARNET-ASUS	false
197.192.154.251	unknown	Egypt		36992	ETISALAT-MISREG	false
165.139.176.150	unknown	United States		11686	ENAUS	false
171.148.60.101	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
88.144.36.106	unknown	United Kingdom		12708	ONETEL-ASTalkTalkCommunications LimitedGB	false
197.210.170.3	unknown	Nigeria		29465	VCG-ASNG	false
95.231.65.178	unknown	Italy		3269	ASN-IBSNAZIT	false
156.215.141.76	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.231.181.95	unknown	Seychelles		26484	IKGUL-26484US	false
41.202.62.185	unknown	South Africa		25818	CMCNETWORKSZA	false
197.131.5.169	unknown	Morocco		6713	IAM-ASMA	false
42.116.150.58	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	false
156.78.164.220	unknown	United States		18862	NCS-HEALTHCAREUS	false
197.87.110.25	unknown	South Africa		10474	OPTINETZA	false
16.156.166.198	unknown	United States		unknown	unknown	false
156.203.180.103	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.55.39.63	unknown	United States		22146	LANDAMUS	false
156.158.25.75	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
156.183.78.33	unknown	Egypt		36992	ETISALAT-MISREG	false
156.7.184.118	unknown	United States		29975	VODACOM-ZA	false
188.19.223.167	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
200.185.26.94	unknown	Brazil		16685	TIVITTERCEIRIZACAODEPROCESSOSSERVETECSABR	false
218.245.176.103	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
148.115.69.203	unknown	United States		6501	SOUTHERNETUS	false
2.202.172.128	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.112.91.25	unknown	Canada		63350	FONCLOUDCA	false
197.165.92.222	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.86.54.155	unknown	South Africa		10474	OPTINETZA	false
156.102.62.18	unknown	United States		393504	XNSTGCA	false
98.105.91.27	unknown	United States		6167	CELLCO-PARTUS	false
73.161.162.133	unknown	United States		7922	COMCAST-7922US	false
41.113.157.210	unknown	South Africa		16637	MTNNS-ASZA	false
156.63.125.78	unknown	United States		19902	NET-STATE-OHIOUS	false
179.247.28.58	unknown	Brazil		26599	TELEFONICABRASILSABR	false
62.150.83.78	unknown	Kuwait		9155	QNETKuwaitKW	false
41.4.60.87	unknown	South Africa		29975	VODACOM-ZA	false

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
201.138.200.133	hhLZAq9Uov	Get hash	malicious	Browse	
41.198.255.152	arm7	Get hash	malicious	Browse	
41.57.232.57	apep.arm	Get hash	malicious	Browse	
156.246.150.168	w66OTKGVFv	Get hash	malicious	Browse	
	U4r9W64doy	Get hash	malicious	Browse	
156.134.83.77	bPAMfuy9oa	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	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
	zju8TB277I	Get hash	malicious	Browse	• 162.213.33.108
	JYWllP5wHP	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
	7qvn4qlmi3	Get hash	malicious	Browse	• 162.213.33.132

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TATACOMM-ASTATACommunicationsformerlyVSNLisLeadingISP	Yoshi.x86-20211110-0350	Get hash	malicious	Browse	• 203.144.121.101
	27xJuvcfMM	Get hash	malicious	Browse	• 121.244.236.127
	byxEpar5Zm	Get hash	malicious	Browse	• 202.54.109.229
	7L38cWaJpW	Get hash	malicious	Browse	• 219.64.111.238
	DvwfkRaTRo	Get hash	malicious	Browse	• 121.244.247.26
	wuyZAnkXB9	Get hash	malicious	Browse	• 219.65.148.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YYcy9gLbBC	Get hash	malicious	Browse	• 115.112.234.192
	rMwxCtXmuJ	Get hash	malicious	Browse	• 121.243.69.171
	fukfKHAGMe	Get hash	malicious	Browse	• 14.142.255.116
	x86-20211103-0152	Get hash	malicious	Browse	• 14.143.23.186
	t7WU0JjLAR	Get hash	malicious	Browse	• 121.244.223.53
	mipsel	Get hash	malicious	Browse	• 121.244.48.198
	anWxzNav9N	Get hash	malicious	Browse	• 203.200.217.215
	1bL17EUgTk	Get hash	malicious	Browse	• 202.54.157.123
	arm7	Get hash	malicious	Browse	• 202.54.157.139
	KfvEoN0wlw	Get hash	malicious	Browse	• 115.112.63.129
	Xb1sM3W7BK	Get hash	malicious	Browse	• 115.111.84.179
	zm8eqQuciR	Get hash	malicious	Browse	• 115.119.111.100
	fzkfNBkz1C	Get hash	malicious	Browse	• 121.244.48.168
	pLpqV3XZ76	Get hash	malicious	Browse	• 115.112.63.121
GIGAINFRASoftbankBBCorpJP	arm	Get hash	malicious	Browse	• 219.63.208.12
	TFiqcmldz5	Get hash	malicious	Browse	• 218.181.74.39
	z0x3n.x86-20211110-2150	Get hash	malicious	Browse	• 126.158.18.108
	z0x3n.arm7-20211110-2150	Get hash	malicious	Browse	• 126.26.48.73
	sora.mpsl	Get hash	malicious	Browse	• 221.83.33.106
	l0vNaPgd6f	Get hash	malicious	Browse	• 218.129.236.192
	8fVDxGRR8S	Get hash	malicious	Browse	• 219.33.187.56
	3ObdCtruss	Get hash	malicious	Browse	• 126.254.59.90
	63BjZ1IcIh	Get hash	malicious	Browse	• 126.240.223.75
	QXFOZ3Cshc	Get hash	malicious	Browse	• 60.109.253.115
	sora.x86	Get hash	malicious	Browse	• 61.245.73.61
	sora.arm7	Get hash	malicious	Browse	• 60.132.89.77
	sora.arm	Get hash	malicious	Browse	• 60.66.177.39
	DVHEnaPp2d	Get hash	malicious	Browse	• 60.93.167.115
	HwcNrhNfZg	Get hash	malicious	Browse	• 126.128.203.128
	X5bKvoLX1E	Get hash	malicious	Browse	• 219.209.94.139
	e9e6i5D2gK	Get hash	malicious	Browse	• 126.89.139.234
	eGH4d5FDoU	Get hash	malicious	Browse	• 220.54.222.144
	hz4vFpTJb8	Get hash	malicious	Browse	• 126.83.241.213
	0LuSWzDmJG	Get hash	malicious	Browse	• 126.67.58.198
airtel-tz-asTZ	arm	Get hash	malicious	Browse	• 197.152.229.163
	ecuuS2WNmQ	Get hash	malicious	Browse	• 156.158.248.163
	dYgJ72oG4f	Get hash	malicious	Browse	• 156.158.49.35
	byxEpar5Zm	Get hash	malicious	Browse	• 197.152.229.157
	wsVomvavHj	Get hash	malicious	Browse	• 156.158.50.52
	y2NMF6ulOI	Get hash	malicious	Browse	• 197.152.229.150
	sora.arm	Get hash	malicious	Browse	• 156.159.153.6
	zJk9UEOnQ7	Get hash	malicious	Browse	• 156.158.50.68
	TlhOKlVSwf	Get hash	malicious	Browse	• 156.158.51.130
	eFsSvDKams	Get hash	malicious	Browse	• 156.158.51.118
	KHSQ48GkGn	Get hash	malicious	Browse	• 156.158.98.11
	Hilix.arm	Get hash	malicious	Browse	• 156.158.248.174
	Hilix.x86	Get hash	malicious	Browse	• 156.158.50.70
	oiHTZaiKnI	Get hash	malicious	Browse	• 156.158.50.45
	arm	Get hash	malicious	Browse	• 156.158.98.25
	QtNnZoNz75	Get hash	malicious	Browse	• 197.187.71.28
	zju8TB277l	Get hash	malicious	Browse	• 197.152.130.201
	arm	Get hash	malicious	Browse	• 156.158.248.172
	FWsCarsq8Q	Get hash	malicious	Browse	• 156.156.2.91
	tqQd9hibj0	Get hash	malicious	Browse	• 156.158.50.72

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/5368/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:DTdv:Pdv
MD5:	123E8A88210D5C9186E1F5BC01223E18
SHA1:	D3874690DC88C5B35F16FD1E22FD9509F7F7B94F
SHA-256:	1DD2196542EF5185965E6622A861D1654828AAF9A59928D18C9F4C1B3AC59781
SHA-512:	D77DE391A3B38536003D456E2C34225BB4B4CE643F02FFF7F83E0E6CD491D742BED0E922E583602B400A3C25E4C302E2CBD66737629B6C88397503084A15AA33
Malicious:	false
Reputation:	low
Preview:	5368.

/run/systemd/resolve/stub-resolv.conf	
Process:	/tmp/x86
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:	17D0088725EB9991E9EB82E8A3DE0878E45E6F394BBC2AD260AA59C786FF0AD565E145E21256425D1C0ABE15F3ECB402EBB0A6A5E1C2D5BA7A4D95EC93A286 1F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	nameserver 8.8.8.8.nameserver 8.8.4.4.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Eun:Eu
MD5:	E40FA240615445A4AB185E263D5A642E
SHA1:	70F7B46430AB6CF197A5B8ABE61363FD4F189E68
SHA-256:	EEB67D767BFBDB98DBDA2DDDC8F8D369145FCFE1AA4196101A9ABA3B2C613EFE
SHA-512:	150531E1DFB7424978076B749E786ADD712D67367019D2EE9EF0581727D073308F32AA935450AC0DE8884D432A3B306B38AAC2D13EE072663ABEAF994E88EC56
Malicious:	false
Reputation:	low
Preview:	5410.

/var/log/gpu-manager.log	
Process:	/usr/bin/gpu-manager
File Type:	ASCII text
Category:	dropped
Size (bytes):	1515
Entropy (8bit):	4.825813629825568
Encrypted:	false
SSDEEP:	24:wPXXX9uV6BNu3WDF3GF3XFFxFFed2uk2HUvJlfWkpPpx7uvvAdow9555Ro7uRkoT:wPXXXe6vejpeC2HUR5WkpPpcvAdow959
MD5:	7B48386106F00126E44F428D0193E1ED
SHA1:	75F652293B2DE03A845A73B678A5CB7E9701A9F4
SHA-256:	9F60B5D0D5C6F6CB3892E1687D16333F36E3BD450713B00FDF0B2BB90EC7312C
SHA-512:	57D0856EC65558B4A843A4696B644AC3E80B3EA0E6EC1C2FAC7A00015B96EBB2CC30967EB8DEFC3E648E59AC6882F6A4F69468D4B6CD0FD60F9F343C206DBF BC
Malicious:	false

/var/log/gpu-manager.log	
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:Fd/n:n/n
MD5:	5DE88F8B8A42BF20A95C7C449C13D8DE
SHA1:	42E07D8ECA0D77F8445F835510C1C634DC89E74F
SHA-256:	F9615512F25BC98071A42105AA4A18C4FD1E77EE6B8E7B63B60BAB517DC0114A
SHA-512:	5E1C807B5E7CA6E7A27545BE9418C1954AF3DCA07DE61C9768FCC333A13D646D116DF3B4197B1E106B5C0920DA6FB96FBF83C2F0081937163F22B2FA484661D
Malicious:	false
Preview:	5582.

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.965405452553123
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	x86
File size:	42980
MD5:	776097f22f49b5f4c467e2afdee63009
SHA1:	540cb7d95922f31459afb94d6b37827b41bf677e
SHA256:	c817429ed299ec43b67bf47aad81081496d8ab45afe231890bdb564f4bf4db7d
SHA512:	c6d5fc772deae715e61e36aa808314e6acd2c5c7696535cc58e0d4bf6dc12adfd542d8633a685e0527b7111594378f4a6408a1539986deeb9035025550e4e39a
SSDEEP:	768:St/U6LU5Klt+u+ul5BhMGCykxB8kdtObBcedEjUnbcuyD7UGQRjV:q/LhIbykf8ltcedlnouy8GyZ
File Content Preview:	.ELF.....4.....4. ...(.....D...Dm..Dm.....Q.td.....-Z.UPX!.....T.....?..k.l/.j....\.d*nlz.eze {...v..+.....R.....f.....6..}../..'z.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xc0a4f8
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32

ELF header

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	0xc01000	0xc01000	0xa6ec	0xa6ec	4.0789	0x5	R E	0x1000		
LOAD	0xd44	0x8066d44	0x8066d44	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 11, 2021 03:04:22.575949907 CET	192.168.2.23	8.8.8.8	0xf1b4	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Nov 11, 2021 03:04:22.575997114 CET	192.168.2.23	8.8.8.8	0x35b6	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 03:04:22.594293118 CET	8.8.8.8	192.168.2.23	0xf1b4	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)
Nov 11, 2021 03:04:22.594293118 CET	8.8.8.8	192.168.2.23	0xf1b4	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: x86 PID: 5245 Parent PID: 5120

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	/tmp/x86
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5246 Parent PID: 5245

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86

Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5247 Parent PID: 5245

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5249 Parent PID: 5245

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5250 Parent PID: 5245

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5251 Parent PID: 5245

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5252 Parent PID: 5245

General

Start time:	03:03:34

Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5253 Parent PID: 5252

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

File Activities

File Read

Directory Enumerated

Analysis Process: x86 PID: 5254 Parent PID: 5252

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: x86 PID: 5255 Parent PID: 5254

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

File Activities

File Written

Analysis Process: x86 PID: 5256 Parent PID: 5255

General

Start time:	03:03:34

Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5256 Parent PID: 5255

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5257 Parent PID: 5256

General

Start time:	03:03:34
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: 5256

General

Start time:	03:03:34
Start date:	11/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /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 /tmp/x86 /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: x86 PID: 5265 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5265 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /var/log/wtmp"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5266 Parent PID: 5265

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5266 Parent PID: 5265

General

Start time:	03:03:47
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: x86 PID: 5267 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5267 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5268 Parent PID: 5267

General

Start time:	03:03:47
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: 5267

General

Start time:	03:03:47
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: x86 PID: 5269 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5269 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /bin/netstat"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5270 Parent PID: 5269

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5270 Parent PID: 5269

General

Start time:	03:03:47
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: x86 PID: 5271 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5271 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "iptables -F"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5272 Parent PID: 5271

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5272 Parent PID: 5271

General

Start time:	03:03:47
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: x86 PID: 5276 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5276 Parent PID: 5255

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5278 Parent PID: 5276

General

Start time:	03:03:47
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5278 Parent PID: 5276

General

Start time:	03:03:47
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: x86 PID: 5283 Parent PID: 5255

General

Start time:	03:03:49
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5283 Parent PID: 5255

General

Start time:	03:03:49
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 perl"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5284 Parent PID: 5283

General

Start time:	03:03:49
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: 5283

General

Start time:	03:03:49
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: x86 PID: 5285 Parent PID: 5255

General

Start time:	03:03:53
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5285 Parent PID: 5255

General

Start time:	03:03:53
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 python"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5286 Parent PID: 5285

General

Start time:	03:03:53
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5286 Parent PID: 5285

General

Start time:	03:03:53
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: x86 PID: 5289 Parent PID: 5255

General

Start time:	03:03:55
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5289 Parent PID: 5255

General

Start time:	03:03:55
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "service iptables stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5290 Parent PID: 5289

General

Start time:	03:03:55
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5290 Parent PID: 5289

General

Start time:	03:03:56
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: 5292 Parent PID: 5290

General

Start time:	03:03:56
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5292 Parent PID: 5290

General

Start time:	03:03:56
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: 5293 Parent PID: 5290

General

Start time:	03:03:56
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5293 Parent PID: 5290

General

Start time:	03:03:56
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: 5294 Parent PID: 5290

General

Start time:	03:03:56
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5294 Parent PID: 5290

General

Start time:	03:03:56
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: 5295 Parent PID: 5290

General

Start time:	03:03:56
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5296 Parent PID: 5295

General

Start time:	03:03:56
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5296 Parent PID: 5295

General

Start time:	03:03:56
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: 5297 Parent PID: 5295

General

Start time:	03:03:56
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5297 Parent PID: 5295

General

Start time:	03:03:56
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: 5290 Parent PID: 5289

General

Start time:	03:03:59
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: x86 PID: 5300 Parent PID: 5255

General

Start time:	03:03:59
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5300 Parent PID: 5255

General

Start time:	03:03:59
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "/sbin/iptables -F; /sbin/iptables -X"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5301 Parent PID: 5300

General

Start time:	03:03:59
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5301 Parent PID: 5300

General

Start time:	03:03:59
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: 5302 Parent PID: 5300

General

Start time:	03:03:59
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5302 Parent PID: 5300

General

Start time:	03:03:59
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: x86 PID: 5303 Parent PID: 5255

General

Start time:	03:03:59
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5303 Parent PID: 5255

General

Start time:	03:03:59
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "service firewalld stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5304 Parent PID: 5303

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5304 Parent PID: 5303

General

Start time:	03:04:00
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: 5305 Parent PID: 5304

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5305 Parent PID: 5304

General

Start time:	03:04:00
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: 5306 Parent PID: 5304

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5306 Parent PID: 5304

General

Start time:	03:04:00
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: 5307 Parent PID: 5304

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5307 Parent PID: 5304

General

Start time:	03:04:00
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: 5308 Parent PID: 5304

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/usr/sbin/service

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

Analysis Process: service PID: 5309 Parent PID: 5308

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5309 Parent PID: 5308

General

Start time:	03:04:00
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: 5310 Parent PID: 5308

General

Start time:	03:04:00
Start date:	11/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5310 Parent PID: 5308

General

Start time:	03:04:00
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: 5304 Parent PID: 5303

General

Start time:	03:04:02
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: x86 PID: 5311 Parent PID: 5255

General

Start time:	03:04:03
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5311 Parent PID: 5255

General

Start time:	03:04:03
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf ~/.bash_history"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5312 Parent PID: 5311

General

Start time:	03:04:03
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5312 Parent PID: 5311

General

Start time:	03:04:03
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: x86 PID: 5313 Parent PID: 5255

General

Start time:	03:04:03
Start date:	11/11/2021
Path:	/tmp/x86
Arguments:	n/a
File size:	42980 bytes
MD5 hash:	776097f22f49b5f4c467e2afdee63009

Analysis Process: sh PID: 5313 Parent PID: 5255

General

Start time:	03:04:03
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	sh -c "history -c"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5337 Parent PID: 1

General

Start time:	03:04:21
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5337 Parent PID: 1

General

Start time:	03:04:21
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: 5367 Parent PID: 1

General

Start time:	03:04:25
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5367 Parent PID: 1

General

Start time:	03:04:25
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: 5368 Parent PID: 1

General

Start time:	03:04:25
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5368 Parent PID: 1

General

Start time:	03:04:25
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: 5371 Parent PID: 1320

General

Start time:	03:04:32
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5371 Parent PID: 1320

General

Start time:	03:04:32
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: 5372 Parent PID: 1320

General

Start time:	03:04:32
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5372 Parent PID: 1320

General

Start time:	03:04:32
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: 5375 Parent PID: 1

General

Start time:	03:04:32
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: 5375 Parent PID: 1

General

Start time:	03:04:32
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: 5410 Parent PID: 1860

General

Start time:	03:04:53

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

Analysis Process: pulseaudio PID: 5410 Parent PID: 1860

General

Start time:	03:04:53
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 Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5435 Parent PID: 1

General

Start time:	03:04:58
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: 5435 Parent PID: 1

General

Start time:	03:04:58
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: 5436 Parent PID: 5435

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5436 Parent PID: 5435

General

Start time:	03:04:58
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: 5437 Parent PID: 5436

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5437 Parent PID: 5436

General

Start time:	03:04:58
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: 5438 Parent PID: 5435

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5438 Parent PID: 5435

General

Start time:	03:04:58
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: 5439 Parent PID: 5438

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5439 Parent PID: 5438

General

Start time:	03:04:58
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: 5440 Parent PID: 5435

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5440 Parent PID: 5435

General

Start time:	03:04:58
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: 5441 Parent PID: 5440

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5441 Parent PID: 5440

General

Start time:	03:04:58
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: 5442 Parent PID: 5435

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5442 Parent PID: 5435

General

Start time:	03:04:58
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: 5443 Parent PID: 5442

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5443 Parent PID: 5442

General

Start time:	03:04:58
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: 5444 Parent PID: 5435

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5444 Parent PID: 5435

General

Start time:	03:04:58
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: 5445 Parent PID: 5444

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5445 Parent PID: 5444

General

Start time:	03:04:58
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: 5446 Parent PID: 5435

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5446 Parent PID: 5435

General

Start time:	03:04:58
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: 5447 Parent PID: 5446

General

Start time:	03:04:58
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5447 Parent PID: 5446

General

Start time:	03:04:58
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: 5451 Parent PID: 5435

General

Start time:	03:05:00
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5451 Parent PID: 5435

General

Start time:	03:05:00
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: 5452 Parent PID: 5451

General

Start time:	03:05:00
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5452 Parent PID: 5451

General

Start time:	03:05:00
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: 5453 Parent PID: 5435

General

Start time:	03:05:00
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5453 Parent PID: 5435

General

Start time:	03:05:00
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: 5454 Parent PID: 5453

General

Start time:	03:05:00
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5454 Parent PID: 5453

General

Start time:	03:05:00

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: 5455 Parent PID: 1

General

Start time:	03:05:00
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: 5455 Parent PID: 1

General

Start time:	03:05:00
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: 5456 Parent PID: 5455

General

Start time:	03:05:00
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: 5456 Parent PID: 5455

General

Start time:	03:05:00
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: 5457 Parent PID: 1

General

Start time:	03:05:02
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: 5457 Parent PID: 1

General

Start time:	03:05:02
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: 5462 Parent PID: 2038

General

Start time:	03:05:06
Start date:	11/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5462 Parent PID: 2038

General

Start time:	03:05:06
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: 5475 Parent PID: 1

General

Start time:	03:05:11
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: 5475 Parent PID: 1

General

Start time:	03:05:11
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: 5502 Parent PID: 1

General

Start time:	03:05:12
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5502 Parent PID: 1

General

Start time:	03:05:12
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: 5553 Parent PID: 1

General

Start time:	03:06:44
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: 5553 Parent PID: 1

General

Start time:	03:06:44
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: 5554 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5554 Parent PID: 5553

General

Start time:	03:06:44
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: 5555 Parent PID: 5554

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5555 Parent PID: 5554

General

Start time:	03:06:44
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: 5556 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5556 Parent PID: 5553

General

Start time:	03:06:44
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: 5557 Parent PID: 5556

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5557 Parent PID: 5556

General

Start time:	03:06:44
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: 5558 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5558 Parent PID: 5553

General

Start time:	03:06:44
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: 5559 Parent PID: 5558

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5559 Parent PID: 5558

General

Start time:	03:06:44
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: 5560 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5560 Parent PID: 5553

General

Start time:	03:06:44
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: 5561 Parent PID: 5560

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5561 Parent PID: 5560

General

Start time:	03:06:44
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: 5562 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5562 Parent PID: 5553

General

Start time:	03:06:44
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: 5563 Parent PID: 5562

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5563 Parent PID: 5562

General

Start time:	03:06:44
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: 5564 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5564 Parent PID: 5553

General

Start time:	03:06:44
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: 5565 Parent PID: 5564

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5565 Parent PID: 5564

General

Start time:	03:06:44
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: 5566 Parent PID: 5553

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5566 Parent PID: 5553

General

Start time:	03:06:44
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: 5567 Parent PID: 5566

General

Start time:	03:06:44
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5567 Parent PID: 5566

General

Start time:	03:06:44
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: 5568 Parent PID: 5553

General

Start time:	03:06:45
Start date:	11/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5568 Parent PID: 5553

General

Start time:	03:06:45
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: 5569 Parent PID: 5568

General

Start time:	03:06:45
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5569 Parent PID: 5568

General

Start time:	03:06:45
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: 5570 Parent PID: 1

General

Start time:	03:06:46
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: 5570 Parent PID: 1

General

Start time:	03:06:46
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: 5571 Parent PID: 5570

General

Start time:	03:06:46
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: 5571 Parent PID: 5570

General

Start time:	03:06:46
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: 5574 Parent PID: 1

General

Start time:	03:06:48
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: 5574 Parent PID: 1

General

Start time:	03:06:48
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: 5582 Parent PID: 1

General

Start time:	03:06:58
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5582 Parent PID: 1

General

Start time:	03:06:58
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