ID: 528759
Sample Name: SadGbSEaaD
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 18:38:57
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

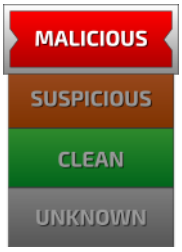
Linux Analysis Report SadGbSEaaD

Overview

General Information

Sample Name:	SadGbSEaaD
Analysis ID:	528759
MD5:	031afe8b5c0562d.
SHA1:	7ab79aaa20d216..
SHA256:	8a2b9ef42d6da1c.
Tags:	32 elf mips mirai
Infos:	

Detection

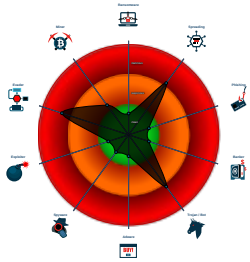


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Sample tries to kill many processes…
- Deletes all firewall rules
- Sample deletes itself
- Sample is packed with UPX
- Deletes security-related log files
- Sample reads /proc/mounts (often u…
- Executes the "kill" or "pkill" comman…
- Sample contains only a LOAD segm…
- Reads CPU information from /sys in…
- Yara signature match
- Executes the "grep" command used…

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528759
Start date:	25.11.2021
Start time:	18:38:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SadGbSEaaD
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:	mal72.spre.troj.evad.lin@0/9@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- SadGbSEaaD (PID: 5222, Parent: 5119, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/SadGbSEaaD
  - SadGbSEaaD New Fork (PID: 5224, Parent: 5222)
  - SadGbSEaaD New Fork (PID: 5225, Parent: 5222)
    - SadGbSEaaD New Fork (PID: 5230, Parent: 5225)
    - SadGbSEaaD New Fork (PID: 5232, Parent: 5225)
      - SadGbSEaaD New Fork (PID: 5234, Parent: 5232)
        - SadGbSEaaD New Fork (PID: 5236, Parent: 5234)

- sh (PID: 5236, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
  - sh New Fork (PID: 5238, Parent: 5236)
  - rm (PID: 5238, Parent: 5236, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/SadGbSEaaD /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jlxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
- SadGbSEaaD New Fork (PID: 5245, Parent: 5234)
- sh (PID: 5245, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /var/log/wtmp"
  - sh New Fork (PID: 5247, Parent: 5245)
  - rm (PID: 5247, Parent: 5245, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
- SadGbSEaaD New Fork (PID: 5248, Parent: 5234)
- sh (PID: 5248, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/*"
  - sh New Fork (PID: 5250, Parent: 5248)
  - rm (PID: 5250, Parent: 5248, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
- SadGbSEaaD New Fork (PID: 5251, Parent: 5234)
- sh (PID: 5251, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /bin/netstat"
  - sh New Fork (PID: 5253, Parent: 5251)
  - rm (PID: 5253, Parent: 5251, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
- SadGbSEaaD New Fork (PID: 5255, Parent: 5234)
- sh (PID: 5255, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -F"
  - sh New Fork (PID: 5261, Parent: 5255)
  - iptables (PID: 5261, Parent: 5255, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -F
- SadGbSEaaD New Fork (PID: 5265, Parent: 5234)
- sh (PID: 5265, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 busybox"
  - sh New Fork (PID: 5267, Parent: 5265)
  - pkill (PID: 5267, Parent: 5265, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
- SadGbSEaaD New Fork (PID: 5268, Parent: 5234)
- sh (PID: 5268, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 perl"
  - sh New Fork (PID: 5270, Parent: 5268)
  - pkill (PID: 5270, Parent: 5268, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
- SadGbSEaaD New Fork (PID: 5273, Parent: 5234)
- sh (PID: 5273, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 python"
  - sh New Fork (PID: 5275, Parent: 5273)
  - pkill (PID: 5275, Parent: 5273, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
- SadGbSEaaD New Fork (PID: 5276, Parent: 5234)
- sh (PID: 5276, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service iptables stop"
  - sh New Fork (PID: 5278, Parent: 5276)
  - service (PID: 5278, Parent: 5276, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service iptables stop
    - service New Fork (PID: 5279, Parent: 5278)
    - basename (PID: 5279, Parent: 5278, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
    - service New Fork (PID: 5280, Parent: 5278)
    - basename (PID: 5280, Parent: 5278, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
    - service New Fork (PID: 5281, Parent: 5278)
    - systemctl (PID: 5281, Parent: 5278, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
    - service New Fork (PID: 5282, Parent: 5278)
      - service New Fork (PID: 5283, Parent: 5282)
      - systemctl (PID: 5283, Parent: 5282, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
      - service New Fork (PID: 5284, Parent: 5282)
      - sed (PID: 5284, Parent: 5282, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
  - systemctl (PID: 5278, Parent: 5276, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop iptables.service
- SadGbSEaaD New Fork (PID: 5288, Parent: 5234)
- sh (PID: 5288, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "/sbin/iptables -F; /sbin/iptables -X"
  - sh New Fork (PID: 5290, Parent: 5288)
  - iptables (PID: 5290, Parent: 5288, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -F
  - sh New Fork (PID: 5291, Parent: 5288)
  - iptables (PID: 5291, Parent: 5288, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -X
- SadGbSEaaD New Fork (PID: 5292, Parent: 5234)
- sh (PID: 5292, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service firewalld stop"
  - sh New Fork (PID: 5294, Parent: 5292)
  - service (PID: 5294, Parent: 5292, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service firewalld stop
    - service New Fork (PID: 5295, Parent: 5294)
    - basename (PID: 5295, Parent: 5294, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
    - service New Fork (PID: 5296, Parent: 5294)
    - basename (PID: 5296, Parent: 5294, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
    - service New Fork (PID: 5297, Parent: 5294)
    - systemctl (PID: 5297, Parent: 5294, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
    - service New Fork (PID: 5298, Parent: 5294)
      - service New Fork (PID: 5299, Parent: 5298)
      - systemctl (PID: 5299, Parent: 5298, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
      - service New Fork (PID: 5300, Parent: 5298)
      - sed (PID: 5300, Parent: 5298, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
  - systemctl (PID: 5294, Parent: 5292, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop firewalld.service
- SadGbSEaaD New Fork (PID: 5301, Parent: 5234)
- sh (PID: 5301, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf ~/.bash_history"
  - sh New Fork (PID: 5303, Parent: 5301)
  - rm (PID: 5303, Parent: 5301, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /root/.bash_history
- SadGbSEaaD New Fork (PID: 5304, Parent: 5234)

        - sh (PID: 5304, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "history -c"
        - SadGbSEaaD New Fork (PID: 5306, Parent: 5234)
        - SadGbSEaaD New Fork (PID: 5308, Parent: 5234)
- systemd New Fork (PID: 5339, Parent: 1)
- whoopsie (PID: 5339, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5347, Parent: 1)
- sshd (PID: 5347, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5348, Parent: 1)
- sshd (PID: 5348, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5351, Parent: 1320)
- Default (PID: 5351, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5371, Parent: 1320)
- Default (PID: 5371, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5372, Parent: 1)
- accounts-daemon (PID: 5372, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
- systemd New Fork (PID: 5386, Parent: 1860)
- pulseaudio (PID: 5386, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5410, Parent: 1)
- gpu-manager (PID: 5410, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5411, Parent: 5410)
    - sh (PID: 5411, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5412, Parent: 5411)
        - grep (PID: 5412, Parent: 5411, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5413, Parent: 5410)
    - sh (PID: 5413, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5414, Parent: 5413)
        - grep (PID: 5414, Parent: 5413, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5415, Parent: 5410)
    - sh (PID: 5415, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5416, Parent: 5415)
        - grep (PID: 5416, Parent: 5415, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5417, Parent: 5410)
    - sh (PID: 5417, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5418, Parent: 5417)
        - grep (PID: 5418, Parent: 5417, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5419, Parent: 5410)
    - sh (PID: 5419, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5420, Parent: 5419)
        - grep (PID: 5420, Parent: 5419, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5421, Parent: 5410)
    - sh (PID: 5421, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5422, Parent: 5421)
        - grep (PID: 5422, Parent: 5421, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5423, Parent: 5410)
    - sh (PID: 5423, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5424, Parent: 5423)
        - grep (PID: 5424, Parent: 5423, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5425, Parent: 5410)
    - sh (PID: 5425, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
        - sh New Fork (PID: 5426, Parent: 5425)
        - grep (PID: 5426, Parent: 5425, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5427, Parent: 1)
- generate-config (PID: 5427, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
    - generate-config New Fork (PID: 5428, Parent: 5427)
    - pkill (PID: 5428, Parent: 5427, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5429, Parent: 1)
- gdm-wait-for-drm (PID: 5429, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- gvfsd-fuse New Fork (PID: 5433, Parent: 2038)
- fusermount (PID: 5433, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5443, Parent: 1)
- systemd-user-runtime-dir (PID: 5443, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5464, Parent: 1)
- gdm3 (PID: 5464, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- systemd New Fork (PID: 5511, Parent: 1)
- gpu-manager (PID: 5511, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
    - gpu-manager New Fork (PID: 5512, Parent: 5511)
    - sh (PID: 5512, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
        - sh New Fork (PID: 5513, Parent: 5512)
        - grep (PID: 5513, Parent: 5512, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*$ /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: 5514, Parent: 5511)
    - sh (PID: 5514, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"

- sh New Fork (PID: 5515, Parent: 5514)
  - grep (PID: 5515, Parent: 5514, 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: 5516, Parent: 5511)
- sh (PID: 5516, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5517, Parent: 5516)
  - grep (PID: 5517, Parent: 5516, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5518, Parent: 5511)
- sh (PID: 5518, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5519, Parent: 5518)
  - grep (PID: 5519, Parent: 5518, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*$ /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: 5520, Parent: 5511)
- sh (PID: 5520, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5521, Parent: 5520)
  - grep (PID: 5521, Parent: 5520, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5522, Parent: 5511)
- sh (PID: 5522, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5523, Parent: 5522)
  - grep (PID: 5523, Parent: 5522, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*$ /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: 5524, Parent: 5511)
- sh (PID: 5524, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
  - sh New Fork (PID: 5525, Parent: 5524)
  - grep (PID: 5525, Parent: 5524, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5526, Parent: 5511)
- sh (PID: 5526, Parent: 5511, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
  - sh New Fork (PID: 5527, Parent: 5526)
  - grep (PID: 5527, Parent: 5526, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*$ /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: 5528, Parent: 1)
- generate-config (PID: 5528, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
  - generate-config New Fork (PID: 5529, Parent: 5528)
  - pkill (PID: 5529, Parent: 5528, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- systemd New Fork (PID: 5531, Parent: 1)
- gdm-wait-for-drm (PID: 5531, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- systemd New Fork (PID: 5537, Parent: 1)
- gdm3 (PID: 5537, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
- **cleanup**

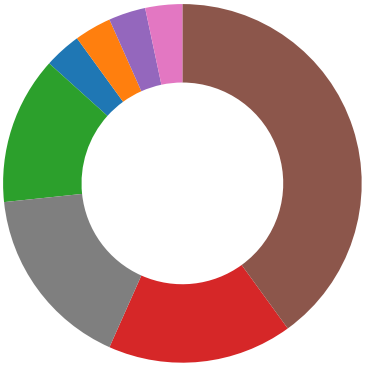
Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SadGbSEaaD	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xc7b0:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xc81f:$s2: $Id: UPX • 0xc7d0:$s3: $Info: This file is packed with the UPX executable packer

Jbx Signature Overview

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



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Deletes all firewall rules

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

Malware Analysis System Evasion:

Deletes security-related log files

Mitre Att&ck Matrix

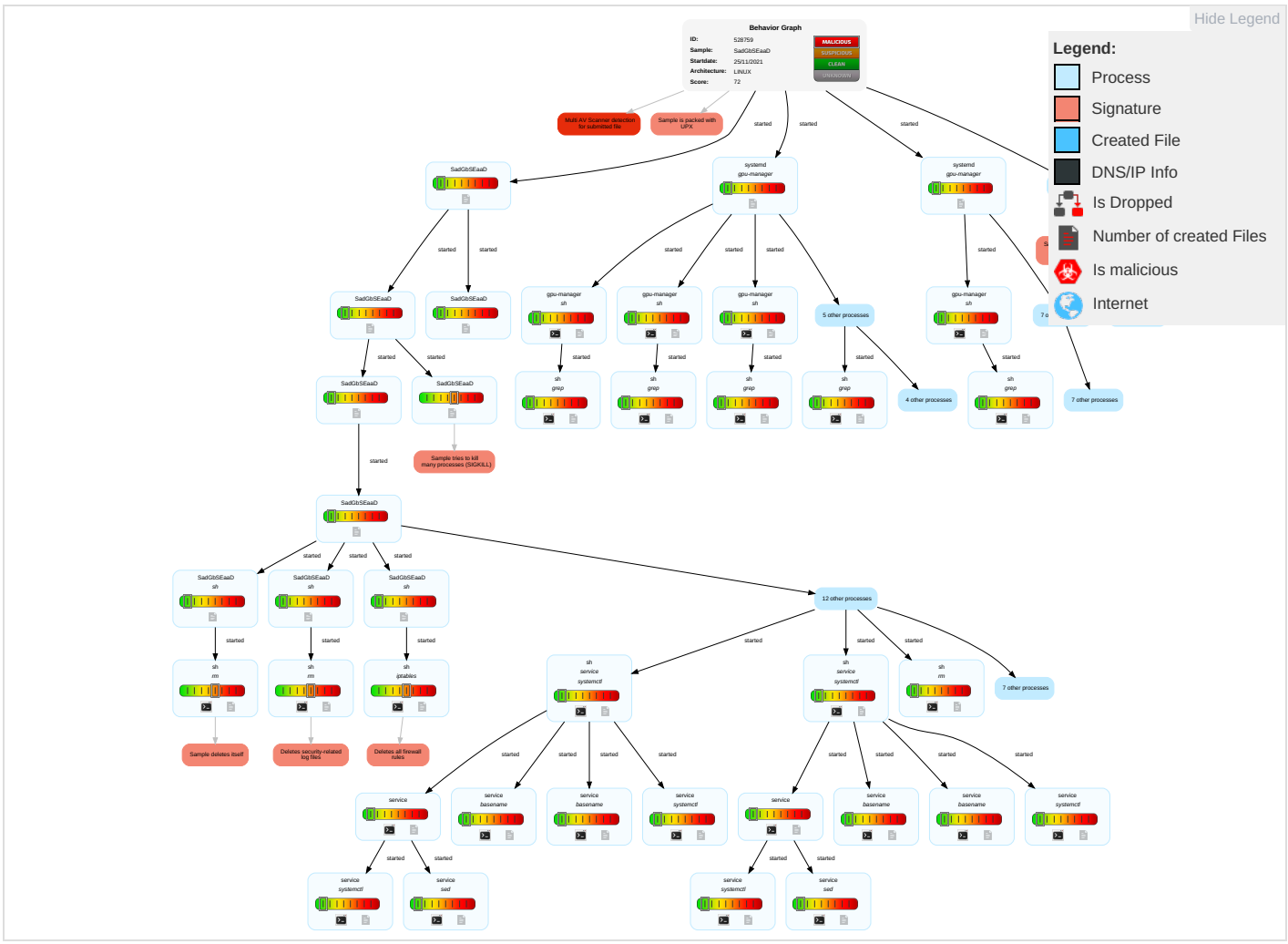
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Path Interception	File and Directory Permissions Modification 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatio
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Network Configuration Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
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	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Disable or Modify System Firewall 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Indicator Removal on Host 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SadGbSEaaD	20%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

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:	3:5bkrlZsXvn:pkckv
MD5:	28FE6435F34B3367707BB1C5D5F6B430
SHA1:	EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6
SHA-256:	721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0
SHA-512:	6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.monitor.

/proc/5348/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:DRdvn:Ndvn
MD5:	3EF34F121A6567F0BA4BA91ECBCF02A1
SHA1:	4717E42F13939A385C9A56661B962D1F681C0794
SHA-256:	F9BEE384387E79153F170D318A737CD21F09629D44688ECDC52AC31E128C2745
SHA-512:	93D1D18FEA49E589C8AD4D435F78850C7AD2FA3A3F1F7857B9E82AAD27C768913C16B947E8311FF04B57024B36FAEE30A8CEA8B6B7B73D8B20B01F694BAA2260
Malicious:	false
Reputation:	low
Preview:	5348.

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

/run/user/1000/pulse/pid	
SSDEEP:	3:DdTv:BTv
MD5:	2A1CA5B92D3768BE40B6336FC569FE4A
SHA1:	48462E8B308EC176015059A662E552217D2D6772
SHA-256:	B5E361F8FC7EBEF020A876B4AF8F041B8C3403703E0E23AD3D1DF6CF3048203E
SHA-512:	27532A8BFA1874038B2F61C971F4864BE8D824FAD134E7B1B03237851EDA8993958DAC27E023C52EF84AF0B18768347439A6DC51D4AD9B3EA62E90A9F806D420
Malicious:	false
Reputation:	low
Preview:	5386.

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

/var/run/gdm3.pid	
Process:	/usr/sbin/gdm3
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:FWc:D
MD5:	F4AC5F432DDDC207F126ADBDB69F5B77
SHA1:	85779FD856ADA77F77CAEF8E4E1A7B1C21731774
SHA-256:	52D3411459C6C6E2CAEAD9A1232A2E52763124432AF69BAB58A16EB714B61A62
SHA-512:	82F4B59D28655CA2555634CD4C1D6AB0F56FFE04E408B70CAA47BB164D16778B6D02DD50798EAA55548E95454C7D3DB87B51125123982E4A44872909A7A021F3
Malicious:	false
Preview:	5537.

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.958921028701868
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	SadGbSEaaD
File size:	53364
MD5:	031afe8b5c0562d8f256cd4c1ba70eac
SHA1:	7ab79aaa20d216648c6197e89e02e7244511c326
SHA256:	8a2b9ef42d6da1cf4216252b5d5354013c439a9cd88ac99 2a1c953b744ef79cd
SHA512:	dd7bf3e0bdaaaf45acd3610ecc87e4b9db65d593b17c386 6f257b245a404d89dfd75415c245b3c863a747f1a45c7dff 1b17fe9d962aedcbacd01e57d317c7e72

General

SSDEEP:	1536:+kZmb1tixCdWslx+XvTdL6/nPnZ1+RdSk5V8U:+aO1lQvTR6/Pn+Rdx
File Content Preview:	.ELF.....4.....4. ...(.....=...=.....F...F.....i`UPX!`.....V.....?.E.h;....#.....b.L#<p.....1.....)B..R...Ov.....P.y...TU@.q..M.....-..Lt..q.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x10bc00
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
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	0x100000	0x100000	0xcf3d	0xcf3d	4.1175	0x5	R E	0x10000		
LOAD	0xe9cc	0x46e9cc	0x46e9cc	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: SadGbSEaaD PID: 5222 Parent PID: 5119

General

Start time:	18:39:41
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	/tmp/SadGbSEaaD
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5224 Parent PID: 5222

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SadGbSEaaD PID: 5225 Parent PID: 5222

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SadGbSEaaD PID: 5230 Parent PID: 5225

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: SadGbSEaaD PID: 5232 Parent PID: 5225

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SadGbSEaaD PID: 5234 Parent PID: 5232

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Written

Analysis Process: SadGbSEaaD PID: 5236 Parent PID: 5234

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5236 Parent PID: 5234

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5238 Parent PID: 5236

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5238 Parent PID: 5236

General

Start time:	18:39:42
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/SadGbSEaaD /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jlxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Directory Enumerated

Analysis Process: SadGbSEaaD PID: 5245 Parent PID: 5234

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5245 Parent PID: 5234

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /var/log/wtmp"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5247 Parent PID: 5245

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5247 Parent PID: 5245

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /var/log/wtmp
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: SadGbSEaaD PID: 5248 Parent PID: 5234

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5248 Parent PID: 5234

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5250 Parent PID: 5248

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5250 Parent PID: 5248

General

Start time:	18:39:54
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/*
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: SadGbSEaaD PID: 5251 Parent PID: 5234

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5251 Parent PID: 5234

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /bin/netstat"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5253 Parent PID: 5251

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5253 Parent PID: 5251

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /bin/netstat
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: SadGbSEaaD PID: 5255 Parent PID: 5234

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5255 Parent PID: 5234

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "iptables -F"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5261 Parent PID: 5255

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5261 Parent PID: 5255

General

Start time:	18:39:55
Start date:	25/11/2021
Path:	/usr/sbin/iptables
Arguments:	iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5265 Parent PID: 5234

General

Start time:	18:39:56
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5265 Parent PID: 5234

General

Start time:	18:39:56
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5267 Parent PID: 5265

General

Start time:	18:39:56
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5267 Parent PID: 5265

General

Start time:	18:39:56
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 busybox
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: SadGbSEaaD PID: 5268 Parent PID: 5234

General

Start time:	18:39:58
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5268 Parent PID: 5234

General

Start time:	18:39:58
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 perl"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5270 Parent PID: 5268

General

Start time:	18:39:58
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5270 Parent PID: 5268

General

Start time:	18:39:58
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 perl
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: SadGbSEaaD PID: 5273 Parent PID: 5234

General

Start time:	18:40:00
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5273 Parent PID: 5234

General

Start time:	18:40:00
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "pkill -9 python"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5275 Parent PID: 5273

General

Start time:	18:40:00
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5275 Parent PID: 5273

General

Start time:	18:40:00
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill -9 python
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: SadGbSEaaD PID: 5276 Parent PID: 5234

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5276 Parent PID: 5234

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "service iptables stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5278 Parent PID: 5276

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5278 Parent PID: 5276

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	service iptables stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: 5279 Parent PID: 5278

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5279 Parent PID: 5278

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5280 Parent PID: 5278

General

Start time:	18:40:04

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

Analysis Process: basename PID: 5280 Parent PID: 5278

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5281 Parent PID: 5278

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5281 Parent PID: 5278

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active multi-user.target
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: service PID: 5282 Parent PID: 5278

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5283 Parent PID: 5282

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5283 Parent PID: 5282

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl list-unit-files --full --type=socket
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Directory Enumerated

Analysis Process: service PID: 5284 Parent PID: 5282

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5284 Parent PID: 5282

General

Start time:	18:40:04
Start date:	25/11/2021
Path:	/usr/bin/sed
Arguments:	sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: systemctl PID: 5278 Parent PID: 5276

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl stop iptables.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5288 Parent PID: 5234

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5288 Parent PID: 5234

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "/sbin/iptables -F; /sbin/iptables -X"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5290 Parent PID: 5288

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5290 Parent PID: 5288

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/sbin/iptables
Arguments:	/sbin/iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: sh PID: 5291 Parent PID: 5288

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5291 Parent PID: 5288

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/sbin/iptables
Arguments:	/sbin/iptables -X
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5292 Parent PID: 5234

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5292 Parent PID: 5234

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "service firewalld stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5294 Parent PID: 5292

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5294 Parent PID: 5292

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	service firewalld stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: 5295 Parent PID: 5294

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5295 Parent PID: 5294

General

Start time:	18:40:07

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

File Activities

File Read

Analysis Process: service PID: 5296 Parent PID: 5294

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5296 Parent PID: 5294

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5297 Parent PID: 5294

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5297 Parent PID: 5294

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active multi-user.target

File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: service PID: 5298 Parent PID: 5294

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: 5299 Parent PID: 5298

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5299 Parent PID: 5298

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl list-unit-files --full --type=socket
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Directory Enumerated

Analysis Process: service PID: 5300 Parent PID: 5298

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/sbin/service
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5300 Parent PID: 5298

General

Start time:	18:40:07
Start date:	25/11/2021
Path:	/usr/bin/sed
Arguments:	sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: systemctl PID: 5294 Parent PID: 5292

General

Start time:	18:40:09
Start date:	25/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl stop firewalld.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5301 Parent PID: 5234

General

Start time:	18:40:09
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5301 Parent PID: 5234

General

Start time:	18:40:09
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf ~/.bash_history"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5303 Parent PID: 5301

General

Start time:	18:40:09
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5303 Parent PID: 5301

General

Start time:	18:40:09
Start date:	25/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /root/.bash_history
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: SadGbSEaaD PID: 5304 Parent PID: 5234

General

Start time:	18:40:10
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: 5304 Parent PID: 5234

General

Start time:	18:40:10
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "history -c"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5306 Parent PID: 5234

General

Start time:	18:40:10
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: SadGbSEaaD PID: 5308 Parent PID: 5234

General

Start time:	18:40:10
Start date:	25/11/2021
Path:	/tmp/SadGbSEaaD
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: systemd PID: 5339 Parent PID: 1

General

Start time:	18:40:28
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5339 Parent PID: 1

General

Start time:	18:40:28
Start date:	25/11/2021
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

Directory Enumerated

Directory Created

Owner / Group Modified

Permission Modified

Analysis Process: systemd PID: 5347 Parent PID: 1

General

Start time:	18:40:32
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5347 Parent PID: 1

General

Start time:	18:40:32
Start date:	25/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5348 Parent PID: 1

General

Start time:	18:40:33
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5348 Parent PID: 1

General

Start time:	18:40:33
Start date:	25/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm3 PID: 5351 Parent PID: 1320

General

Start time:	18:40:40
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5351 Parent PID: 1320

General

Start time:	18:40:40
Start date:	25/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5371 Parent PID: 1320

General

Start time:	18:40:40
Start date:	25/11/2021
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:	18:40:40
Start date:	25/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5372 Parent PID: 1

General

Start time:	18:40:40
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5372 Parent PID: 1

General

Start time:	18:40:40
Start date:	25/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

Analysis Process: systemd PID: 5386 Parent PID: 1860

General

Start time:	18:41:02
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5386 Parent PID: 1860

General

Start time:	18:41:02
Start date:	25/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5410 Parent PID: 1

General

Start time:	18:41:06
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5410 Parent PID: 1

General

Start time:	18:41:06
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

Directory Enumerated

Analysis Process: gpu-manager PID: 5411 Parent PID: 5410

General

Start time:	18:41:06

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

Analysis Process: sh PID: 5411 Parent PID: 5410

General

Start time:	18:41:06
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5412 Parent PID: 5411

General

Start time:	18:41:06
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5412 Parent PID: 5411

General

Start time:	18:41:06
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5413 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5413 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5414 Parent PID: 5413

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5414 Parent PID: 5413

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5415 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5415 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5416 Parent PID: 5415

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5416 Parent PID: 5415

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5417 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5417 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5418 Parent PID: 5417

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5418 Parent PID: 5417

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5419 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5419 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5420 Parent PID: 5419

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5420 Parent PID: 5419

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5421 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5421 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5422 Parent PID: 5421

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5422 Parent PID: 5421

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5423 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5423 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5424 Parent PID: 5423

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5424 Parent PID: 5423

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5425 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5425 Parent PID: 5410

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5426 Parent PID: 5425

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5426 Parent PID: 5425

General

Start time:	18:41:07
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5427 Parent PID: 1

General

Start time:	18:41:08
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5427 Parent PID: 1

General

Start time:	18:41:08
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: generate-config PID: 5428 Parent PID: 5427

General

Start time:	18:41:08
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5428 Parent PID: 5427

General

Start time:	18:41:08
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5429 Parent PID: 1

General

Start time:	18:41:10
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5429 Parent PID: 1

General

Start time:	18:41:10
Start date:	25/11/2021
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities

File Read

Directory Enumerated

Analysis Process: gvfsd-fuse PID: 5433 Parent PID: 2038

General

Start time:	18:41:14
Start date:	25/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5433 Parent PID: 2038

General

Start time:	18:41:14
Start date:	25/11/2021
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

File Activities

File Read

Analysis Process: systemd PID: 5443 Parent PID: 1

General

Start time:	18:41:15
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5443 Parent PID: 1

General

Start time:	18:41:15
Start date:	25/11/2021
Path:	/lib/systemd/systemd-user-runtime-dir
Arguments:	/lib/systemd/systemd-user-runtime-dir stop 1000
File size:	22672 bytes
MD5 hash:	d55f4b0847f88131dbcfb07435178e54

File Activities

File Deleted

File Read

Directory Enumerated

Directory Deleted

Analysis Process: systemd PID: 5464 Parent PID: 1

General

Start time:	18:41:20
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5464 Parent PID: 1

General

Start time:	18:41:20
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes

MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Deleted

File Read

File Written

Directory Created

Owner / Group Modified

Permission Modified

Analysis Process: systemd PID: 5511 Parent PID: 1

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5511 Parent PID: 1

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Analysis Process: gpu-manager PID: 5512 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager

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

Analysis Process: sh PID: 5512 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5513 Parent PID: 5512

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5513 Parent PID: 5512

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5514 Parent PID: 5511

General

Start time:	18:42:51

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

Analysis Process: sh PID: 5514 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5515 Parent PID: 5514

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5515 Parent PID: 5514

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5516 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5516 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5517 Parent PID: 5516

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5517 Parent PID: 5516

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5518 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5518 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5519 Parent PID: 5518

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5519 Parent PID: 5518

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5520 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5520 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5521 Parent PID: 5520

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5521 Parent PID: 5520

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5522 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5522 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5523 Parent PID: 5522

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5523 Parent PID: 5522

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5524 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5524 Parent PID: 5511

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5525 Parent PID: 5524

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5525 Parent PID: 5524

General

Start time:	18:42:51
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 5526 Parent PID: 5511

General

Start time:	18:42:52
Start date:	25/11/2021
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 5526 Parent PID: 5511

General

Start time:	18:42:52
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5527 Parent PID: 5526

General

Start time:	18:42:52
Start date:	25/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5527 Parent PID: 5526

General

Start time:	18:42:52
Start date:	25/11/2021
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5528 Parent PID: 1

General

Start time:	18:42:53
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5528 Parent PID: 1

General

Start time:	18:42:53
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: generate-config PID: 5529 Parent PID: 5528

General

Start time:	18:42:53
Start date:	25/11/2021
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 5529 Parent PID: 5528

General

Start time:	18:42:53
Start date:	25/11/2021
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5531 Parent PID: 1

General

Start time:	18:42:54
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 5531 Parent PID: 1

General

Start time:	18:42:54
Start date:	25/11/2021
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5537 Parent PID: 1

General

Start time:	18:43:05
Start date:	25/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 5537 Parent PID: 1

General

Start time:	18:43:05
Start date:	25/11/2021
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Deleted

File Read

File Written

Directory Created

Owner / Group Modified

Permission Modified