Linux Threat Hunting Case Report
Generated: Sat Jul 5 09:35:57 PM +03 2025

USB Autorun Log:
USB Autorun Log - Sat Jul 5 08:52:31 PM +03 2025

ClamAV Scan:

Port Scan Logs:
Port Scan Log - Sat Jul 5 09:05:52 PM +03 2025
udp 0.0.0.0:5353
udp 0.0.0.0:47100
udp 127.0.0.54:53
udp 127.0.0.53%lo:53
udp [::]:5353
udp [::]:51323
tcp 127.0.0.54:53
tcp 127.0.0.53%lo:53
tcp 127.0.0.1:631
tcp [::1]:631

Suspicious Ports Found:

Suspicious Processes:
Suspicious Process Log -Sat Jul 5 09:19:32 PM +03 2025

Checking for: nc
5 [kworker/R-sync_wq]
1150 /usr/lib/systemd/systemd-timesyncd
1839 /usr/bin/nvidia-persistenced --user nvidia-persistenced --no-persistence-mode --verbose
3130 /usr/libexec/at-spi-bus-launcher
10463 [sd_espeak-ng-mb] <defunct>

Checking for: netcat

Checking for: bash
13742 bash
25142 /bin/bash ./suspicious_process_watch.sh

Checking for: sh
1 /sbin/init splash
6 [kworker/R-slub_flushwq]
1887 /bin/sh /snap/cups/1100/scripts/run-cups-browsed
1888 /bin/sh /snap/cups/1100/scripts/run-cupsd
1890 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
2210 /bin/sh /snap/cups/1100/scripts/run-cups-browsed
3137 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 11 --address=unix:path=/run/user/1000/at-spi/bus_1
3151 /usr/libexec/gcr-ssh-agent --base-dir /run/user/1000/gcr
3220 /usr/bin/gnome-shell
3352 /usr/libexec/gnome-shell-calendar-server
3366 /usr/bin/gjs -m /usr/share/gnome-shell/org.gnome.Shell.Notifications
3416 /usr/libexec/gsd-sharing
3796 /usr/bin/gjs -m /usr/share/gnome-shell/org.gnome.ScreenSaver
3875 /usr/libexec/gvfsd-trash --spawner :1.25 /org/gtk/gvfs/exec_spaw/1
4217 /snap/firefox/6259/usr/lib/firefox/crashhelper 4139 9 /tmp/ 10 12
4310 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -parentBuildID 20250529220913 -prefsHandle 0:37563 -prefMapHandle 1:271480 -sandboxReporter 2 -chrootClient 3 -ipcHandle 4 -initialChannelId {9aabd1a1-e0ef-48d4-8f82-b949aaf15731} -parentPid 4139 -crashReporter 5 -crashHelperPid 4217 -appDir /snap/firefox/6259/usr/lib/firefox/browser 1 socket

```
4343 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:37688 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {487d1ea6-b638-4202-b524-0367fa782162} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 2 tab
4348 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -parentBuildID
20250529220913 -prefsHandle 0:37688 -prefMapHandle 1:271480 -sandboxReporter 2 -
chrootClient 3 -ipcHandle 4 -initialChannelId {374fb48b-ec1e-4c1e-9612-
8ac3310e217e} -parentPid 4139 -crashReporter 5 -crashHelperPid 4217 -appDir
/snap/firefox/6259/usr/lib/firefox/browser 3 rdd
4540 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:47300 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {88293ab3-8ffa-44b4-8c66-d936978f1300} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 4 tab
4649 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -parentBuildID
20250529220913 -sandboxingKind 0 -prefsHandle 0:47464 -prefMapHandle 1:271480 -
sandboxReporter 2 -chrootClient 3 -ipcHandle 4 -initialChannelId {c460b3ca-7051-
474e-ba39-eedaa79b295d} -parentPid 4139 -crashReporter 5 -crashHelperPid 4217 -
appDir /snap/firefox/6259/usr/lib/firefox/browser 5 utility
4715 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42729 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {bfb9fa0f-36f1-4c07-8da3-2085705c39da} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 6 tab
4722 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42729 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {dde1f8f3-3def-4349-becf-2401b9a4cd0e} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 7 tab
4735 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42729 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {e07e2e12-f973-471a-9cdd-76c303ac020f} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 8 tab
10344 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42880 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {3a2c0853-76eb-4c01-ab9c-054357353ca5} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 10 tab
10466 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42880 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {dc531712-d572-4e88-b897-5ee93deb68fd} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
```

```
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 11 tab
10468 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42880 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {df80b300-0750-423d-8999-542ed68541f3} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 12 tab
12418 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42880 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {c64acbb8-1467-4920-844e-c9c1a8fbab04} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 15 tab
13742 bash
16161 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42985 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {2650a7ef-6a38-4bae-bf9f-c5c77decc646} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 17 tab
19991 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42986 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {e4526509-1520-4fe9-b641-e2ae82522575} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 18 tab
22750 /snap/firefox/6259/usr/lib/firefox/firefox -contentproc -isForBrowser -
prefsHandle 0:42987 -prefMapHandle 1:271480 -jsInitHandle 2:245828 -
parentBuildID 20250529220913 -sandboxReporter 3 -chrootClient 4 -ipcHandle 5 -
initialChannelId {3c175da4-b3ea-4909-8bd7-34146196c25a} -parentPid 4139 -
crashReporter 6 -crashHelperPid 4217 -greomni
/snap/firefox/6259/usr/lib/firefox/omni.ja -appomni
/snap/firefox/6259/usr/lib/firefox/browser/omni.ja -appDir
/snap/firefox/6259/usr/lib/firefox/browser 19 tab
23088 [kworker/u64:0-flush-259:0]
23585 gjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -
P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app
25140 sudo ./suspicious_process_watch.sh
25141 sudo ./suspicious_process_watch.sh
25142 /bin/bash ./suspicious_process_watch.sh

Checking for: ncat

Checking for: python
1890 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown
--wait-for-signal

Checking for: perl

Checking for: nmap

Checking for: reverse

Scan Complete. Check ../suspicious_process_log.txt for anything sketchy.
```

File Integrity Check:

Checking: /etc/passwd
Current Hash: 375946863fab152029496047c594fbde20ab597eb9972b90d327e09728b6ed5e
Expected Hash: 375946863fab152029496047c594fbde20ab597eb9972b90d327e09728b6ed5e
File is clean

Checking: /etc/shadow
Current Hash: 97f03b4a856f5f5ae3d169a545f3a6927cb25824262f9f93bbef126a7ab75eef
Expected Hash: 97f03b4a856f5f5ae3d169a545f3a6927cb25824262f9f93bbef126a7ab75eef
File is clean

Checking: /bin/bash
Current Hash: bc5945feb8bd26203ebfafea5ce1878bb2e32cb8fb50ab7ae395cfb1e1aaaef1
Expected Hash: bc5945feb8bd26203ebfafea5ce1878bb2e32cb8fb50ab7ae395cfb1e1aaaef1
File is clean