Removing Adware and Fake Notifications on macOS Monterey

This guide documents the step-by-step process I followed to help a friend clean adware off their MacBook running macOS Monterey.
They were receiving fake alert notifications in Safari and experiencing random shutdowns.
I couldn't access Safari settings in the original user account, so I used a workaround and performed cleanup through a new user account.

Note: Before deleting any files or killing processes, always double-check their legitimacy. Misidentifying a legitimate system process can cause unexpected issues. When in doubt, use tools like VirusTotal or search online for clarification.

Step 1 - Check for Suspicious Startup Items

Before running any tools, I manually checked for signs of malware by inspecting Launch Agents and Daemons. These are common hiding places for persistent malware.

Accessing the Library

- ➔ Open Finder > Go > Home folder.
- ➔ Click **Go** again, then hold the **Option** key and select **Library**.
- ➔ Navigate through these folders and look for suspicious files:
  - ~/Library/LaunchAgents/
  - /Library/LaunchDaemons/
  - /Library/StartupItems/ *(obsolete, but worth checking if present)*

Look out for unfamiliar app names, randomized filenames, or recently modified files and delete if necessary

Known Suspicious Files or Common Adware Names

- ➔ These names may vary slightly or be randomized, but here are some to watch for:
  - Com.pcv.hlpramc.plist
  - com.adobe.fpsaud.plist *(fake version, not legit Flash)*
  - Com.mcp.agent.plist
  - com.avickUpd.plist
  - Com.myppes.download.plist
  - maccleaner.pkg or any "cleaner" tool you didn't install
  - Random strings like com.3gXJ4sd2.random.plist

If in doubt, copy the file name and Google it or upload to VirusTotal.

Step 2 - Use Activity Monitor to Spot Suspicious Processes

Activity Monitor gives a live overview of what's running on the system essential for identifying rogue processes tied to adware or unnecessary background tasks.

- ➔ Open Activity Monitor:
  - ◆ Open Spotlight (Cmd + Space), type Activity Monitor, and hit Enter
  - ◆ Sort by Resource Usage
  - ◆ Go to the CPU tab and sort by % CPU
  - ◆ Go to the Memory tab and look for anything with high memory usage

Take note of processes with strange names or anything using a lot of resources for no clear reason

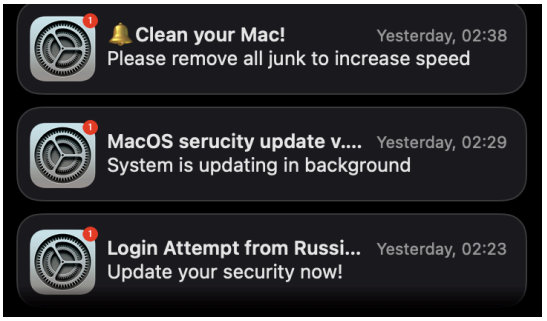
- ➔ **Inspect Unfamiliar Processes**
  - ◆ Right-click the process > Inspect or Sample Process
  - ◆ Google suspicious names or scan on VirusTotal

Don't kill random processes blindly. Use this VirusTotal for analysis and verification especially when combined with what you see in the next steps.

Step 3 - Identify Fake Notifications and Browser Hijacking

Once connected to the internet, the user was getting fake system notifications.

Tip: Many of these pop-ups are from websites granted notification access not from macOS itself. Check for spelling mistakes and weird grammar in the alerts.



I originally thought they were coming from the system, but after a closer look, I noticed the poor spelling and that they only appeared while online, a sign of adware abusing browser notifications.

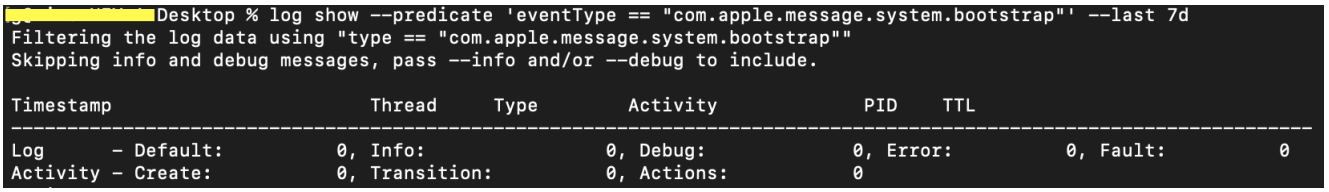
Step 4 - Check System Logs via Terminal

To investigate the source of the notifications, I checked the logs for any unusual system behavior:

- ➔ Open **Terminal**
- ➔ Run the following command to filter logs related to system bootstrapping:

log show --predicate 'eventType == "com.apple.message.system.bootstrap"' --last 7d

What to look for: Unusual system processes, errors, or any suspicious app/process names during the period of fake notifications.



Step 5 - Create a New User Account

Since Safari settings weren't accessible in the original account, I created a new one to bypass the restriction.

- ➔ Go to **System Preferences > Users & Groups**
- ➔ Click the lock to make changes
- ➔ Add a **Standard** or **Admin** account
- ➔ Log into the new account to continue the cleanup safely

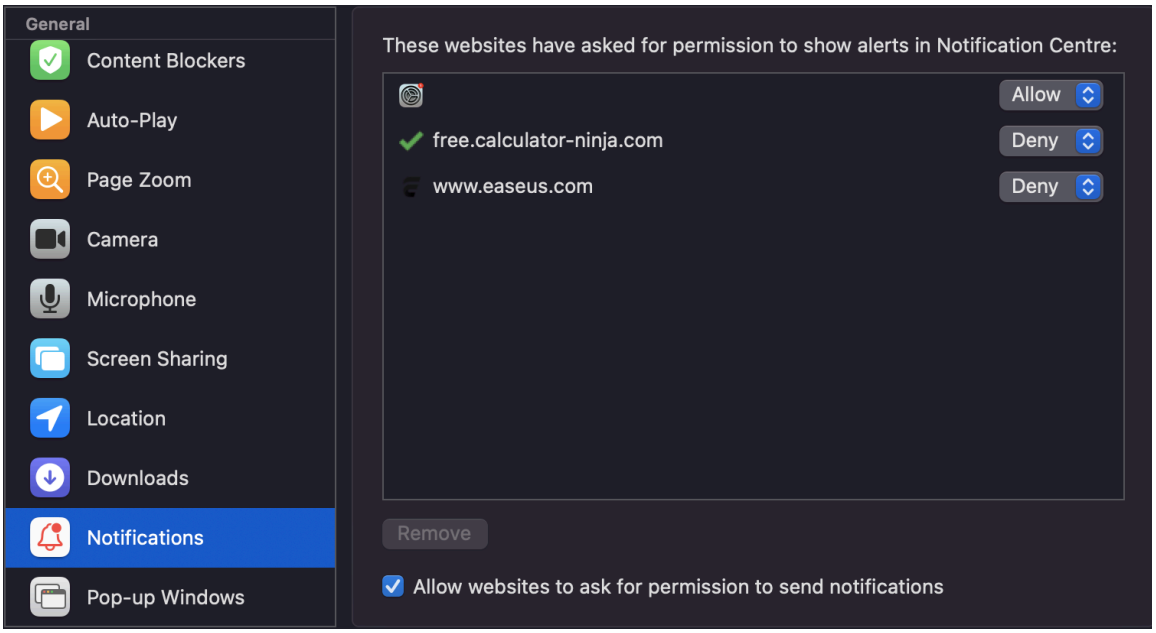
****New User Account bypasses corrupted permissions/extensions in the infected profile. After cleanup, you can delete the temporary user account****

****Performing cleanup from a clean user profile helps avoid interference from active adware processes.****

Step 6 - Clean Up Safari

➔ Remove Suspicious Notification Permissions

- Open **Safari > Preferences > Websites > Notifications**
  Remove any unfamiliar or sketchy websites (in this case, I found 3)



➔ Clear Website Data

- Go to **Safari > Preferences > Privacy > Manage Website Data**
  Click **Remove All** to delete stored cookies and cache

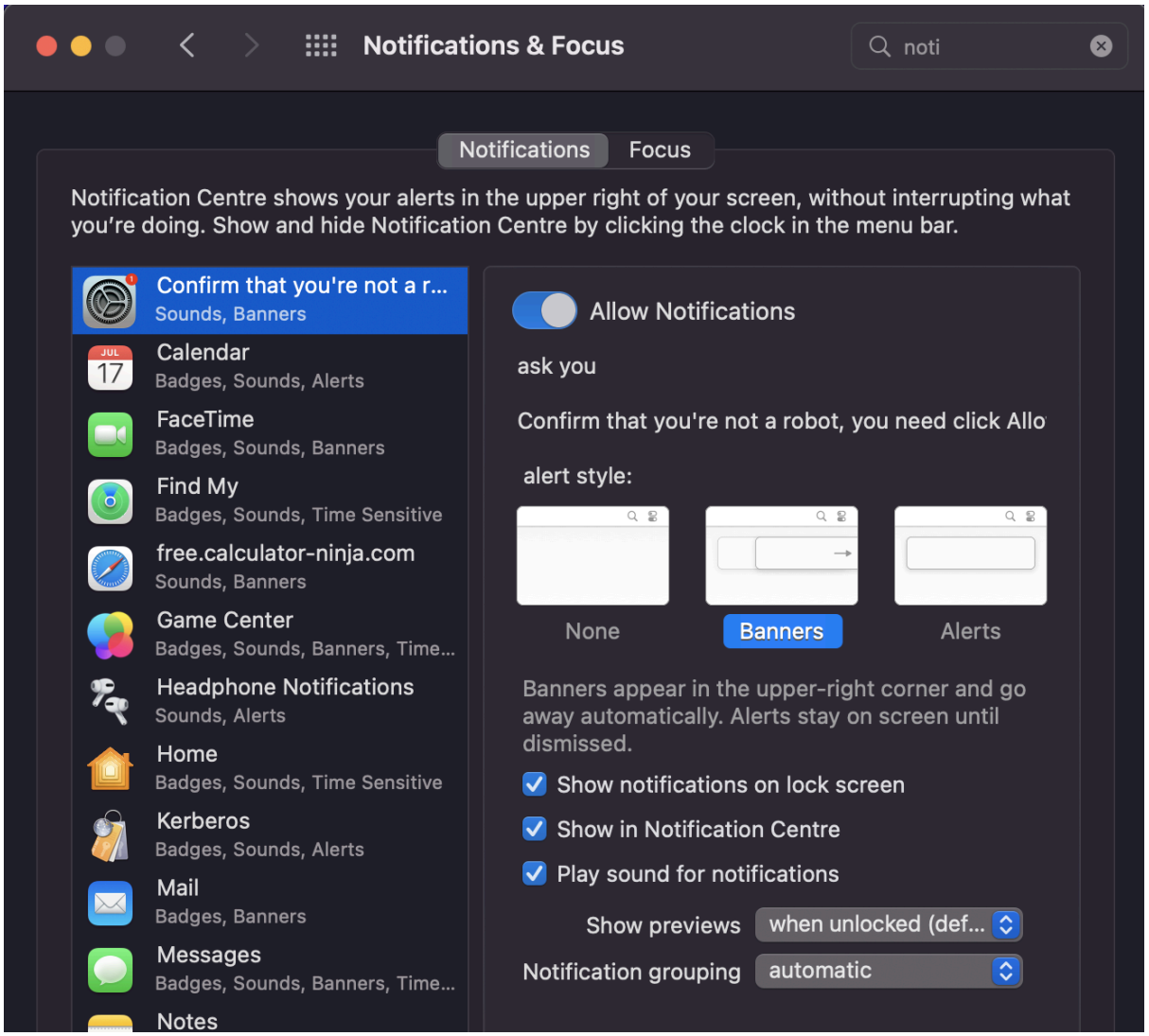
➔ Check Safari Extensions

- Go to **Safari > Preferences > Extensions**
  Disable or uninstall any unknown or untrusted extensions

Step 7 - Check System Settings

Make sure nothing is hiding in Notifications or Login Items:

- ➔ Go to **System Preferences > Notifications & Focus**
  - ◆ Review each app and look for unknown entries
  - ◆ In this case I found the following to be suspicious:
    - Confirm that you are not a robot (fake banner)
    - www.easeus.com
- ➔ Go to **System Preferences > Users & Groups > Login Items**
  - ◆ Remove any suspicious login items



Recheck these after malware scans in case anything respawns.

Step 8 - Run Malware Scan

After manual cleanup, I recommended running a reputable malware removal tool:

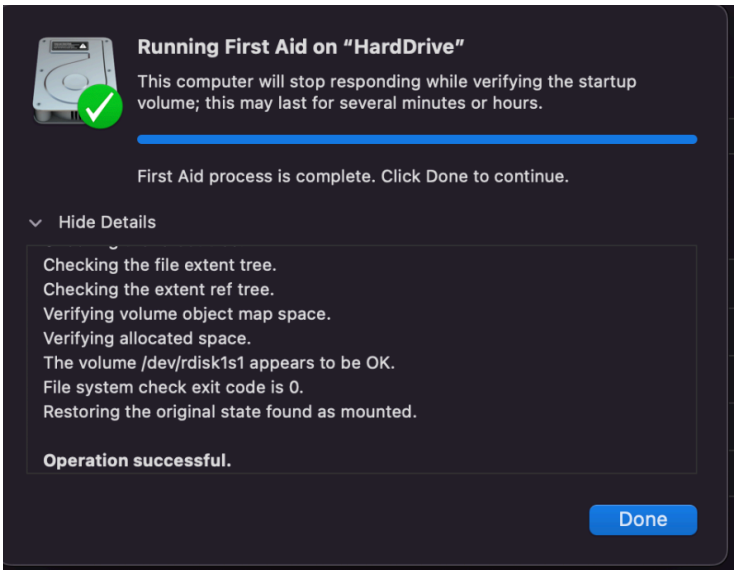
- ➔ Malwarebytes for Mac
- ➔ AdwareMedic (now bundled into Malwarebytes)

These tools help find and remove leftover adware that might be deeper in the system.

Step 9 - Run Disk Utility

To ensure there's no file system damage from the sudden shutdowns:

- ➔ Open Disk Utility via Spotlight
- ➔ Select Macintosh HD and click First Aid > Run
- ➔ Repeat this for any containers or sub-volumes under the main drive.



This is a non-destructive repair tool, so it's safe to run and highly recommended after malware issues.

Step 10 - Run Apple Diagnostics

The user mentioned random shutdowns and a strange screen before the system would freeze.
To rule out hardware issues:

- ➔ Shut down the Mac
- ➔ Turn it on and immediately press and hold the **D** key
- ➔ Wait for Apple Diagnostics to launch
- ➔ Run the test and note any reference codes (e.g., memory or logic board issues)

Important: This test checks for RAM, logic board, SSD, and more it's a key step when dealing with unexplained shutdowns.

Final Checklist

- ☑ ~~Launch Agents/Daemons cleaned~~
- ☑ ~~Safari Notification permissions removed~~
- ☑ ~~Safari Website Data cleared~~
- ☑ ~~Extensions reviewed~~
- ☑ ~~Malware scan completed~~
- ☑ ~~Login Items reviewed~~
- ☑ ~~Notifications & Focus settings checked~~
- ☑ ~~Disk Utility First Aid run~~
- ☑ ~~Apple Diagnostics completed~~

Bonus Tip - Stay Safe Going Forward

To prevent reinfection and stay protected:

- ☐ Avoid clicking pop-ups that claim your Mac is infected or needs urgent attention.
- ☐ Don’t install “cleaning” apps unless you’ve researched and trust them.
- ☐ Keep your macOS and browsers updated to patch known security issues.
- ☐ Review notification permissions regularly in Safari and other browsers.
- ☐ Use an ad-blocker to reduce exposure to malicious ads and fake alerts.
- ☐ Be cautious when downloading apps and always use the official App Store or verified developer websites.

This guide is based on real troubleshooting steps and can serve as a practical reference for helping others facing similar issues on macOS Monterey.

Credits

Guide by Nicolas Cordischi