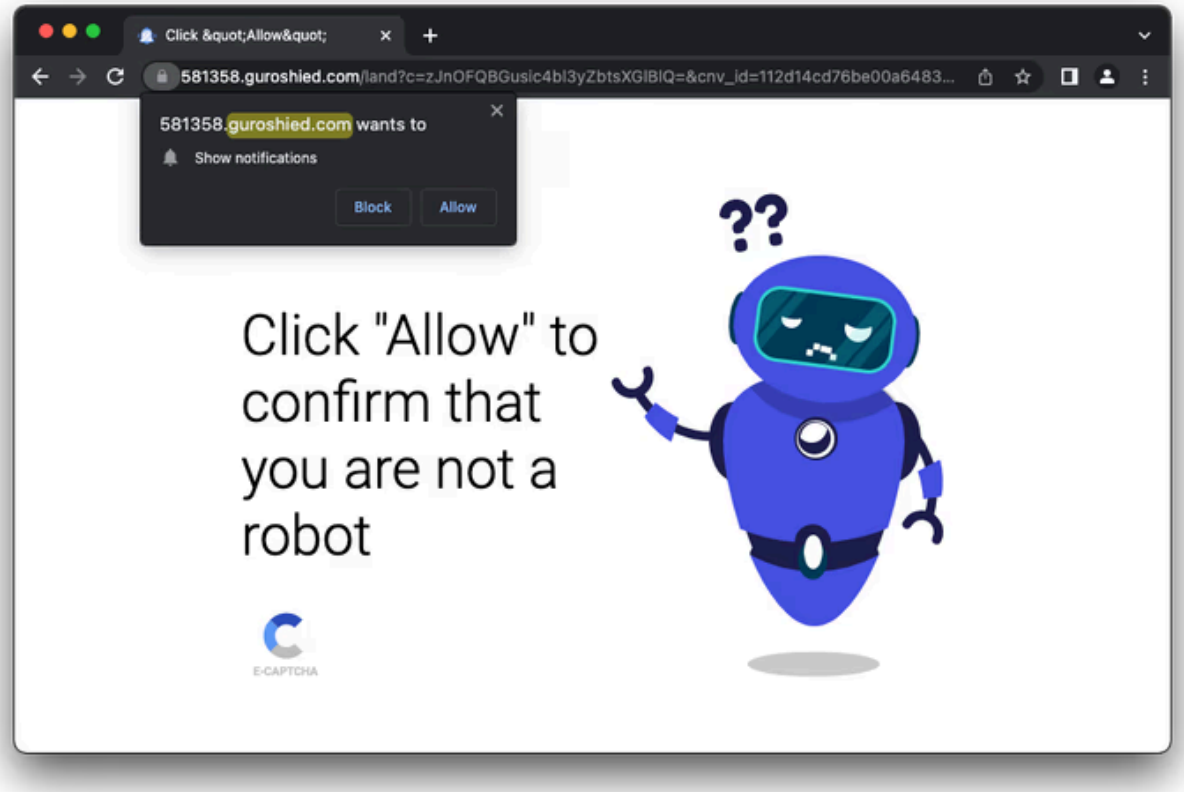
Remove Guroshied virus popup from Mac

By David Balaban

Published: 2024-12-10 · Archived: 2026-04-05 13:24:24 UTC

Staying away from guroshied.com is definitely a good idea because it is a harbor for popup scams, clickbait schemes, and sneaky Mac malware.

Malware campaigns deployed in the macOS ecosystem are rarely as straightforward as hacking computers or injecting dangerous code behind one's back. These plots are increasingly hybrid as they combine social engineering and virus distribution under the umbrella of a multi-step attack chain. The Guroshied hoax is an epitome of this tactic. At the initial stage of the manipulation, Mac users are lured into visiting guroshied.com, a site that displays interactive messages whose real purpose is a far cry from what they say. Once on the hook, the unsuspecting person runs the risk of granting redundant permissions to the shady service. This, in turn, becomes a catalyst for manifold exploitation that runs the gamut from clickbait trickery to outright infestation of the host system with malicious applications.



Those who exercise proper online hygiene may argue that visiting such a fraudulent web page is at odds with basic vigilance. True, but when a user goes there, it's not because they have literally typed the domain name in a browser plus a super-long concatenated string with a bunch of identifiers that denote a specific sub-campaign of

the multifunctional ruse. Instead, people mostly end up on guroshied.com after clicking some eye-catching ad on a popular site. Cybercriminals are very adept at gaming the rules of legitimate services to put their dodgy stuff on them and thereby give their attack surface a boost. One more plausible scenario relies on browser hijackers previously deposited on Macs. These electronic culprits are notoriously effective in terms of tweaking victims' web browsing preferences to organize the web traffic to their advantage.

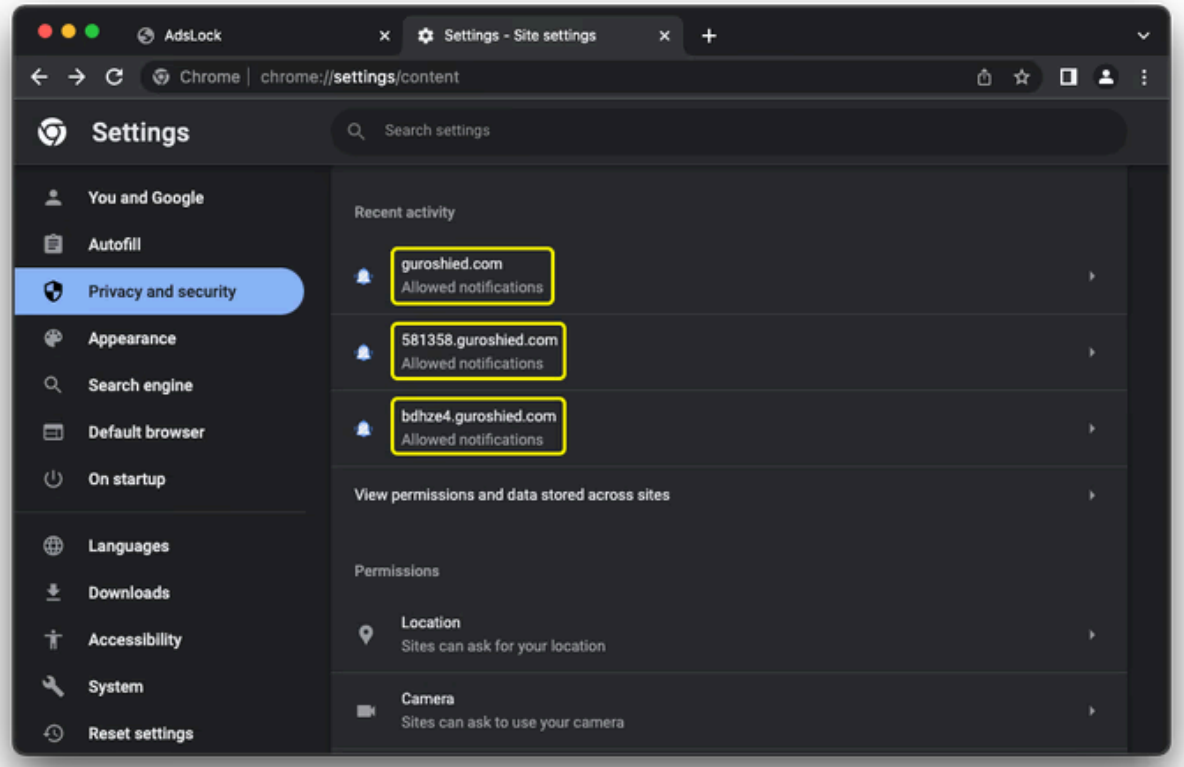
Special Offer

Guroshied popup virus may re-infect your Mac multiple times unless you delete all of its fragments, including hidden ones. Therefore, it is recommended to download Combo Cleaner and scan your system for these stubborn files. **This way, you may reduce the cleanup time from hours to minutes.**

Download Now

Learn how Combo Cleaner works. If the utility spots malicious code, you will need to buy a license to get rid of it.

Putting aside the specific mechanism that brought a user to guroshied.com, the subsequent series of events is a nuisance. There are several landing page designs in the scammers' repertoire. The most common variant mimics garden-variety human verification that's supposedly required to access some useful content. At this point, a major giveaway can be noticed with the naked eye. To confirm that you are not a robot, you are instructed to click an "Allow" button on a popup that says "guroshied.com wants to show notifications". These are completely different things, aren't they? One way or another, the user is one click away from letting classic malvertising activity commence on their Mac. It mishandles web push notifications, a feature used by websites to keep their audiences abreast of new materials they publish.

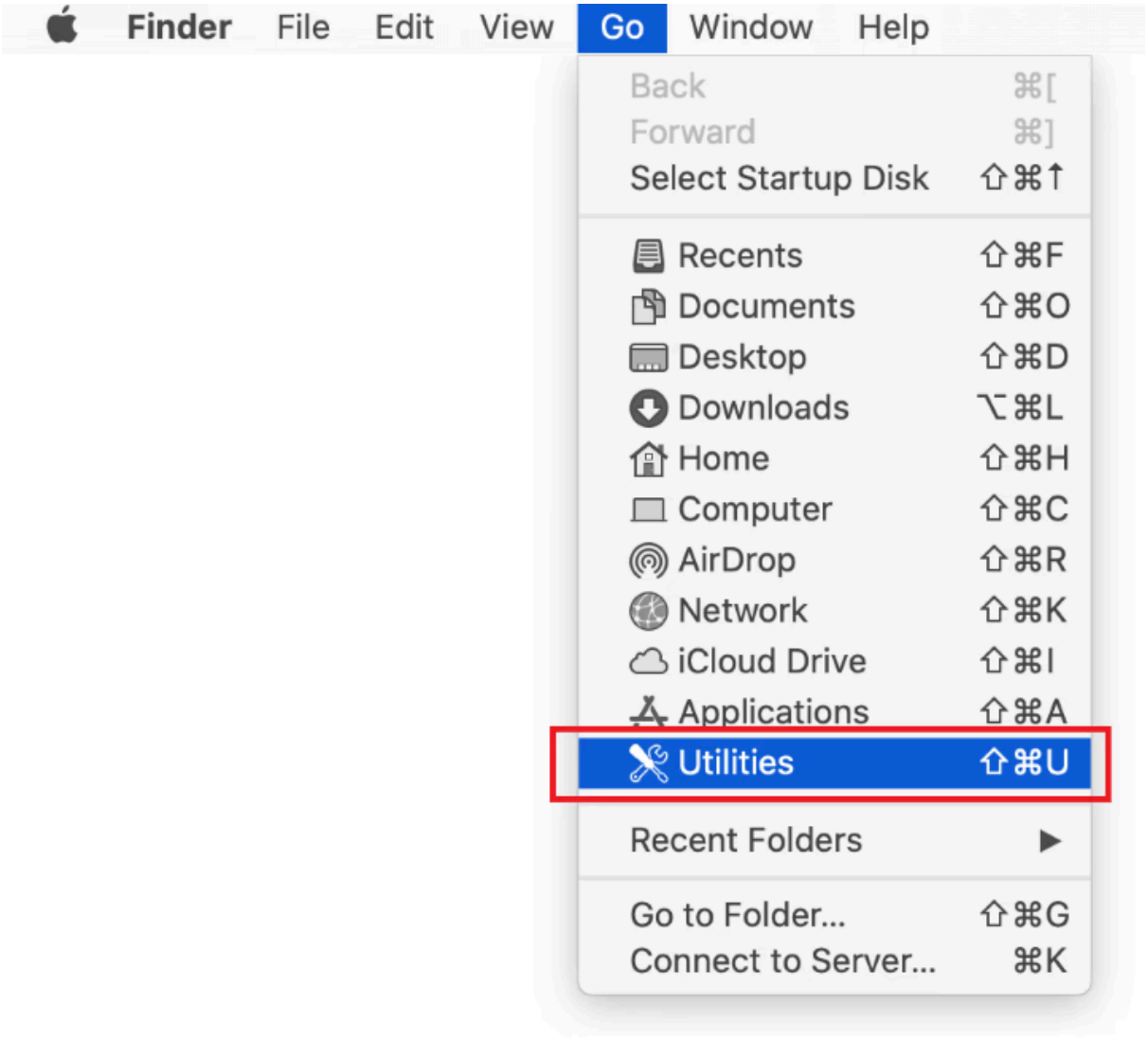


Threat actors have learned to weaponize this technology to deliver sketchy content to users. It turns into a springboard for generating pop-ups that originate from a reconfigured web browser. The worst part is that these ads are also displayed outside the browser. For instance, they will be inundating the top right part of the Mac's desktop, making the victim close an insane number of these pop-ups to see their normal icons and widgets. Another nontrivial risk stems from the contents of these notifications. Most of them contain links that lead to junk sources such as gambling sites or tech support scams. Some will even claim that a virus has been detected on the computer. An example of such imaginary peril is **Trojan_%$@!F**, which is purportedly capable of erasing the operating system.

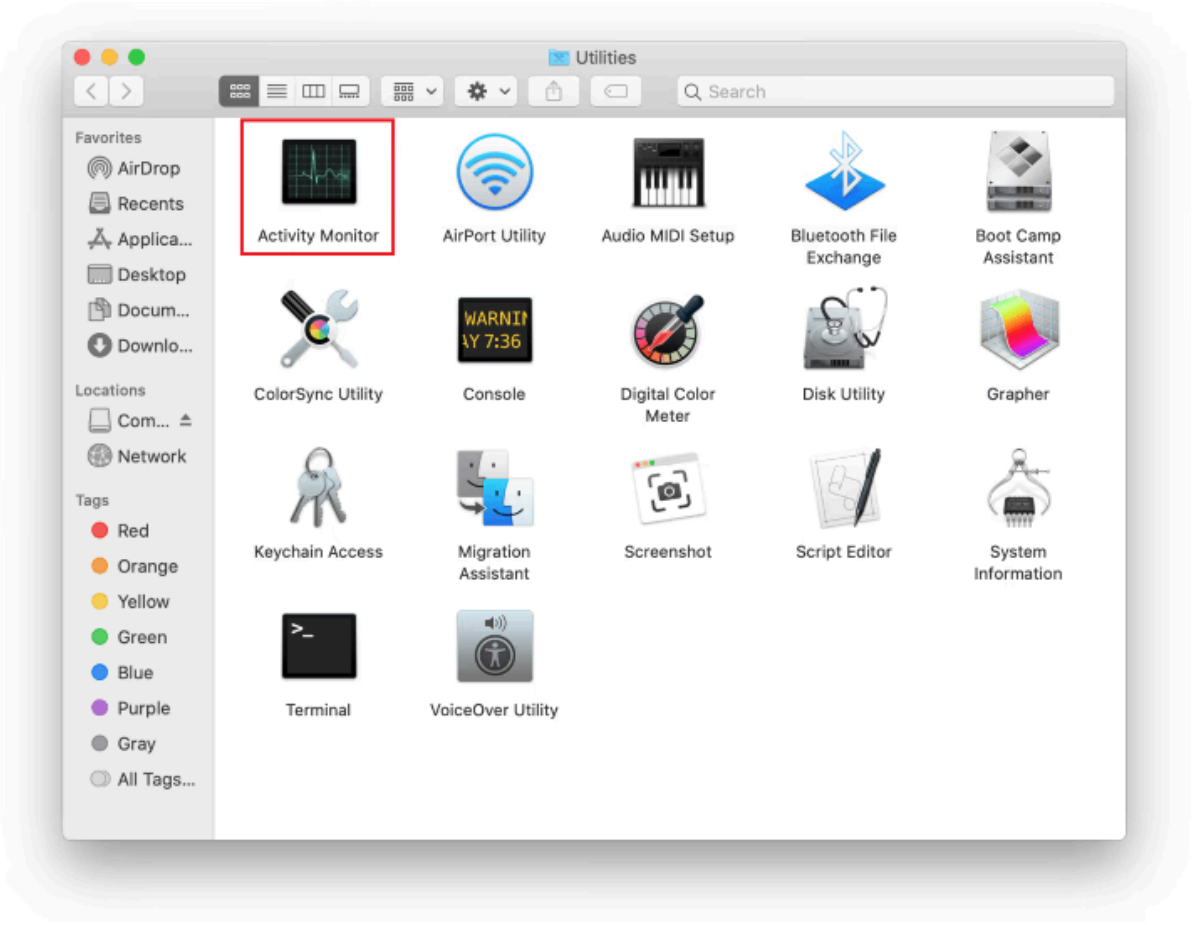
A rule of thumb when dealing with Guroshied virus pop-ups is to avoid clicking them and to ignore what they say because all of it is a lie. However, this is cold comfort for users who will keep getting those annoying notifications regardless. To address this problem for good, you'll need to fix the browser settings and make sure that the fraud is not backed by malware that might have triggered the brainwashing scheme in the first place. In the screenshot above, you can see guroshied.com and several spin-offs (ones with six-character strings prepending the URL) abusing Google Chrome's security and privacy configuration. Notice the "Allowed notifications" tag for each. Resetting these permissions is a good place to start, but it's half the battle. Use the following recommendations to get rid of Guroshied pop-ups completely. Going forward, be sure to take human verification alerts on unfamiliar web pages with a grain of salt.

The steps listed below will walk you through the removal of this malicious application. Be sure to follow the instructions in the specified order.

1. Expand the **Go** menu in your Mac's Finder bar and select **Utilities** as shown below.

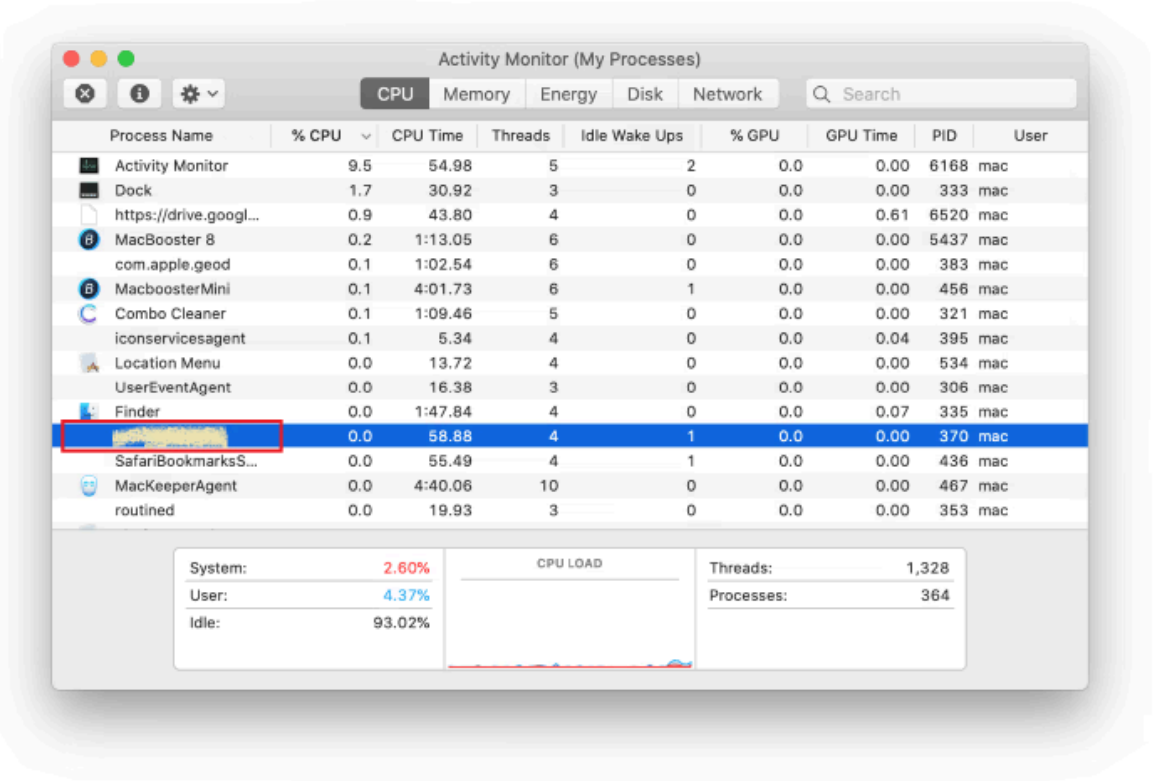


2. Locate the **Activity Monitor** icon on the Utilities screen and double-click on it.

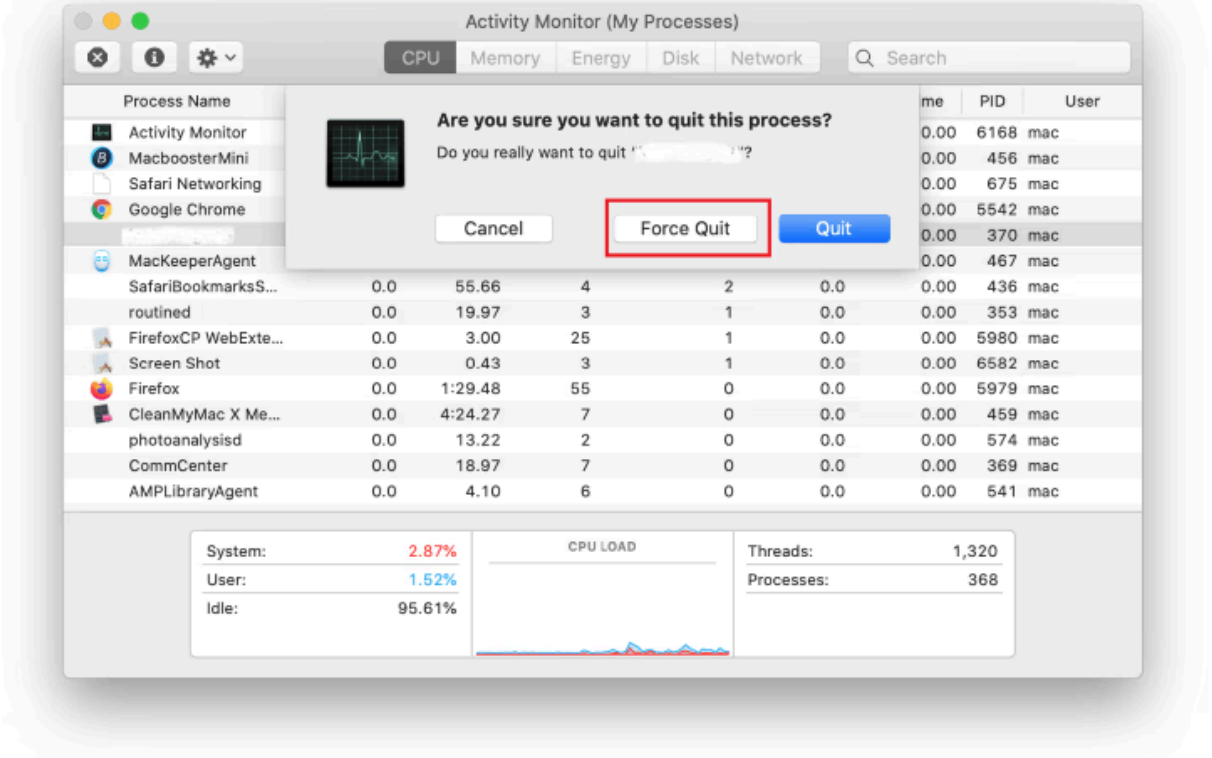


3. In the Activity Monitor app, look for a process that appears suspicious. To narrow down your search, focus on unfamiliar resource-intensive entries on the list. Keep in mind that its name isn't necessarily related to the way the threat is manifesting itself, so you'll need to trust your own judgement. If you pinpoint the

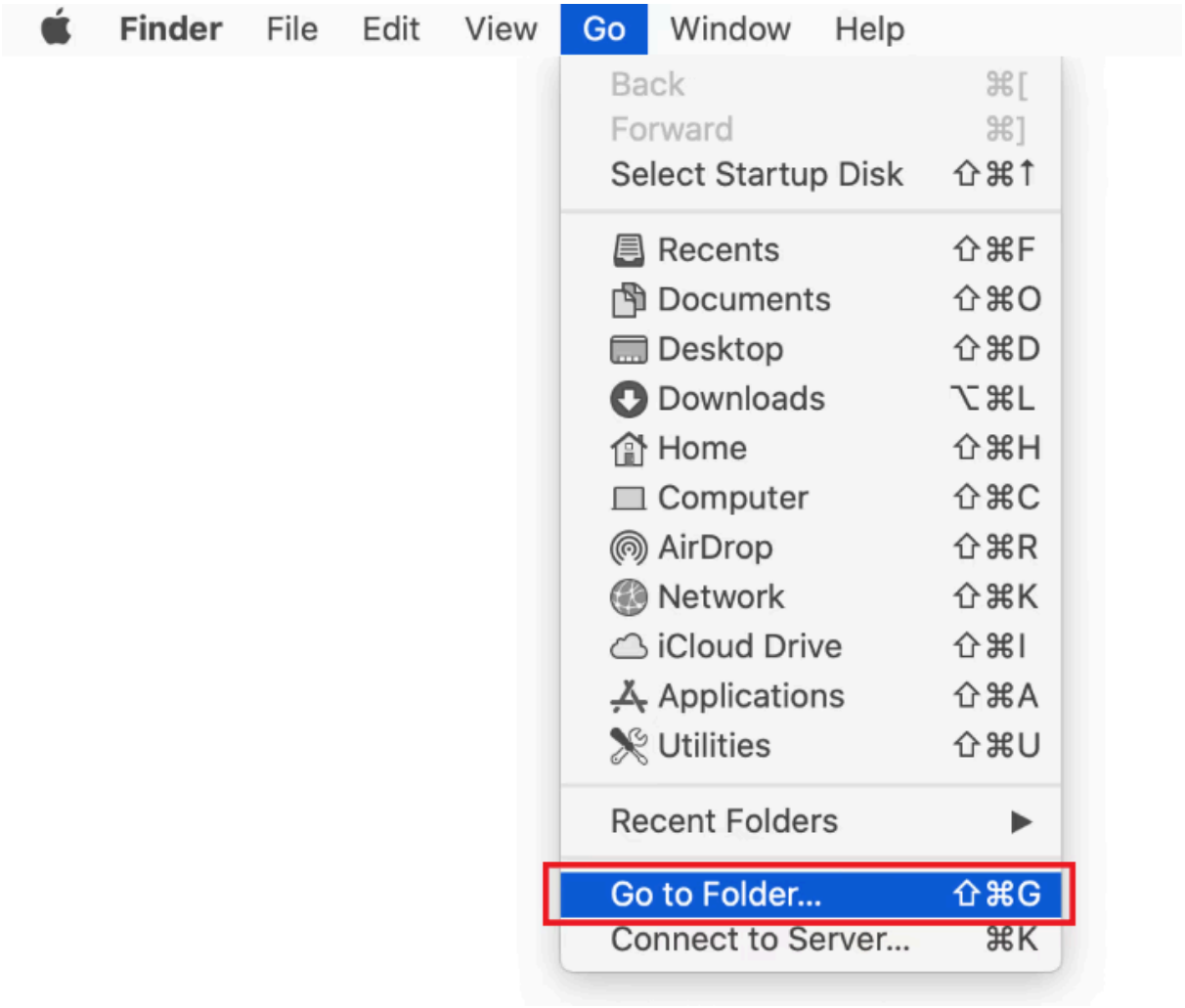
culprit, select it and click on the **Stop** icon in the upper left-hand corner of the screen.



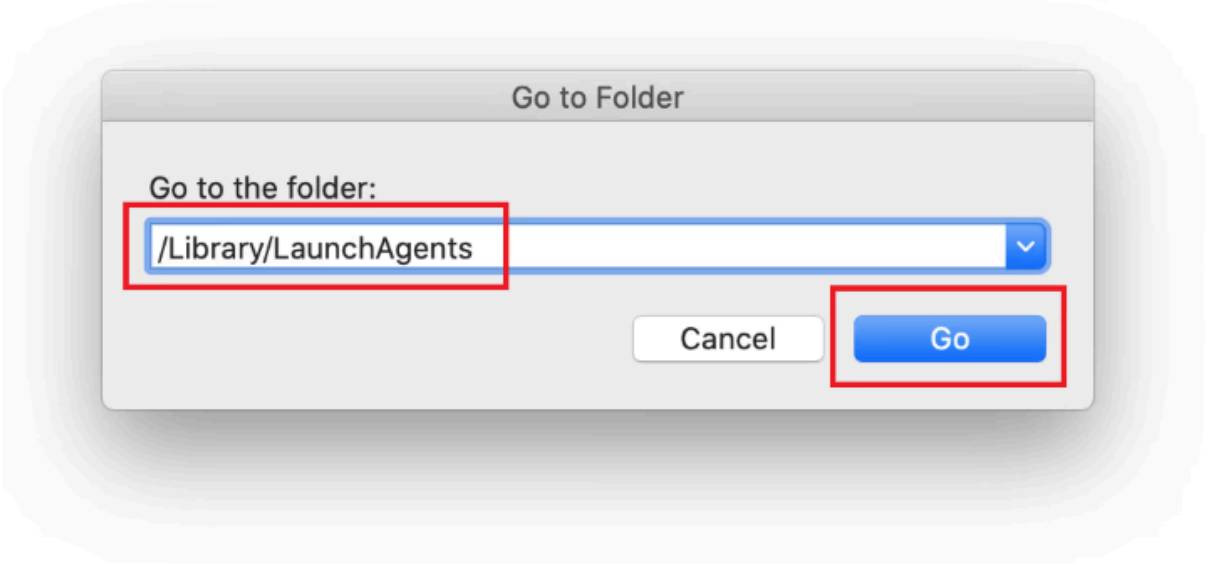
4. When a follow-up dialog pops up asking if you are sure you want to quit the troublemaking process, select the **Force Quit** option.



5. Click on the **Go** menu icon in the Finder again and select **Go to Folder**. You can as well use the **Command-Shift-G** keyboard shortcut.

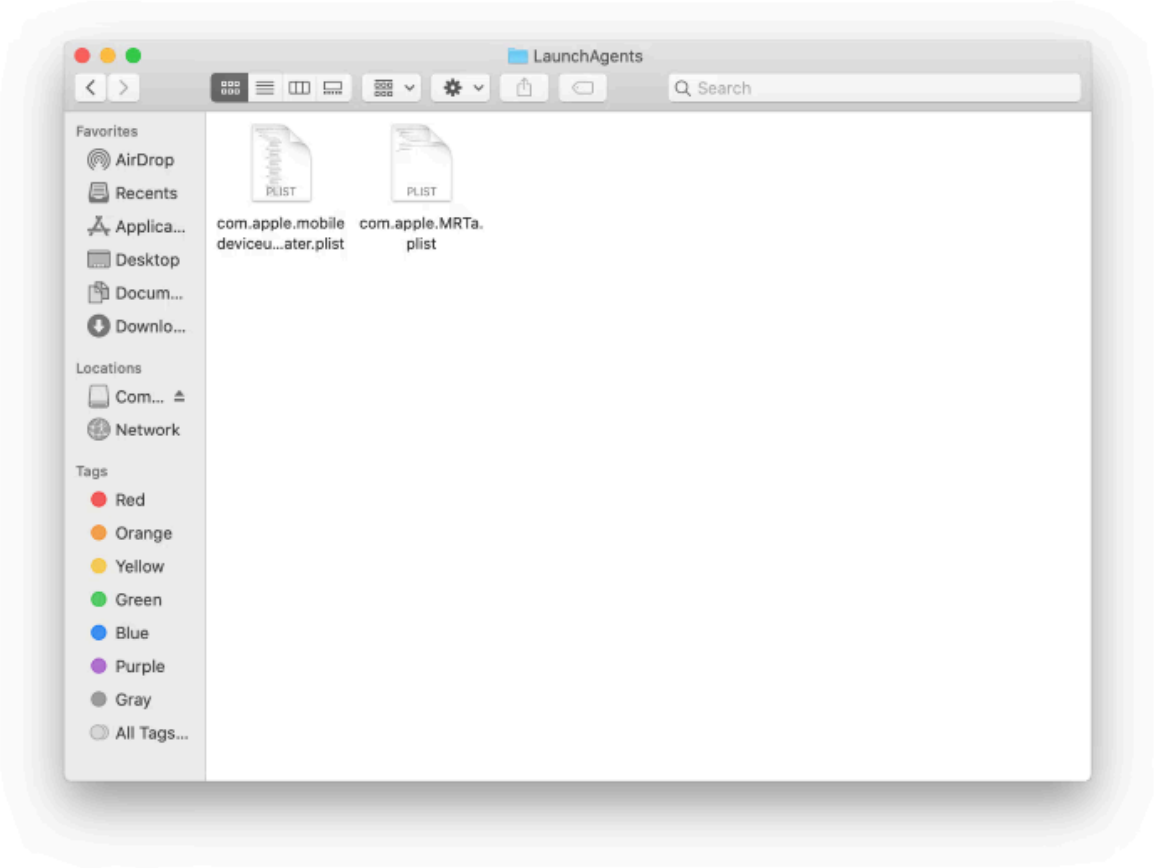


6. Type **/Library/LaunchAgents** in the folder search dialog and click on the **Go** button.

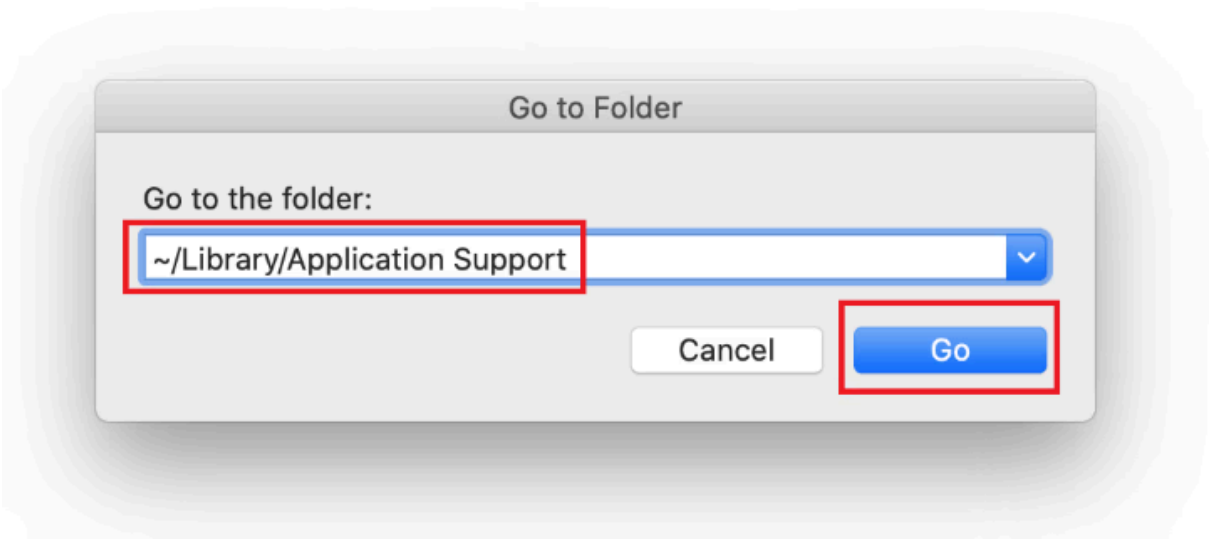


7. Examine the contents of the LaunchAgents folder for dubious-looking items. Be advised that the names of files spawned by malware may give no clear clues that they are malicious, so you should look for recently added entities that appear to deviate from the norm.

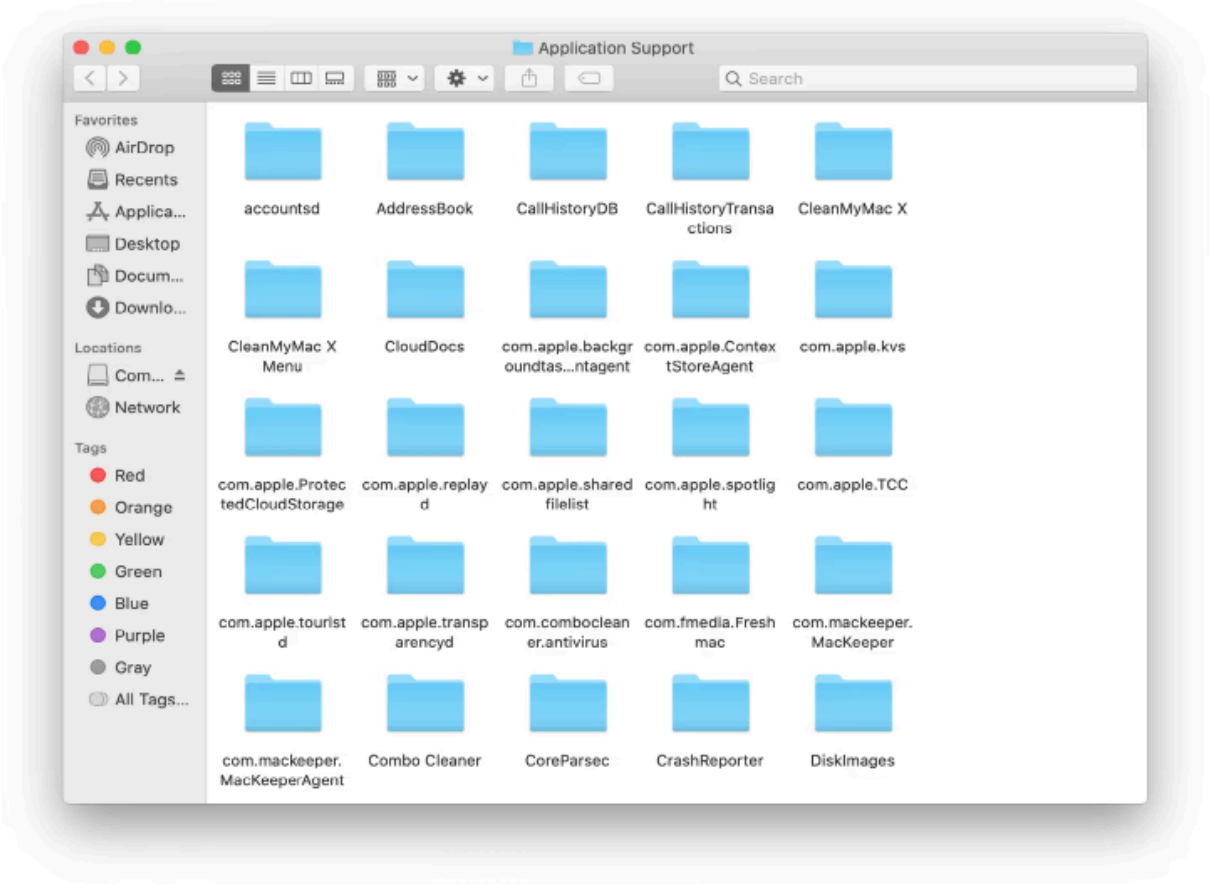
   As an illustration, here are several examples of LaunchAgents related to mainstream Mac infections: **com.updater.mcy.plist**, **com.avickUpd.plist**, and **com.msp.agent.plist**. If you spot files that don't belong on the list, go ahead and drag them to the Trash.



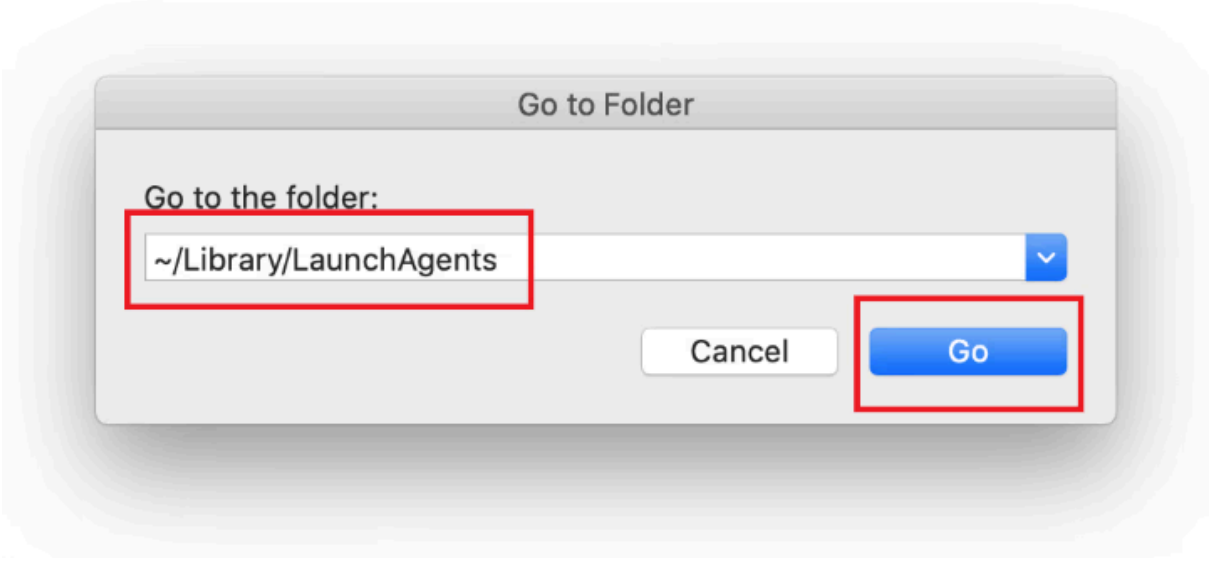
8. Use the **Go to Folder** lookup feature again to navigate to the folder named **~/Library/Application Support** (note the tilde symbol prepended to the path).



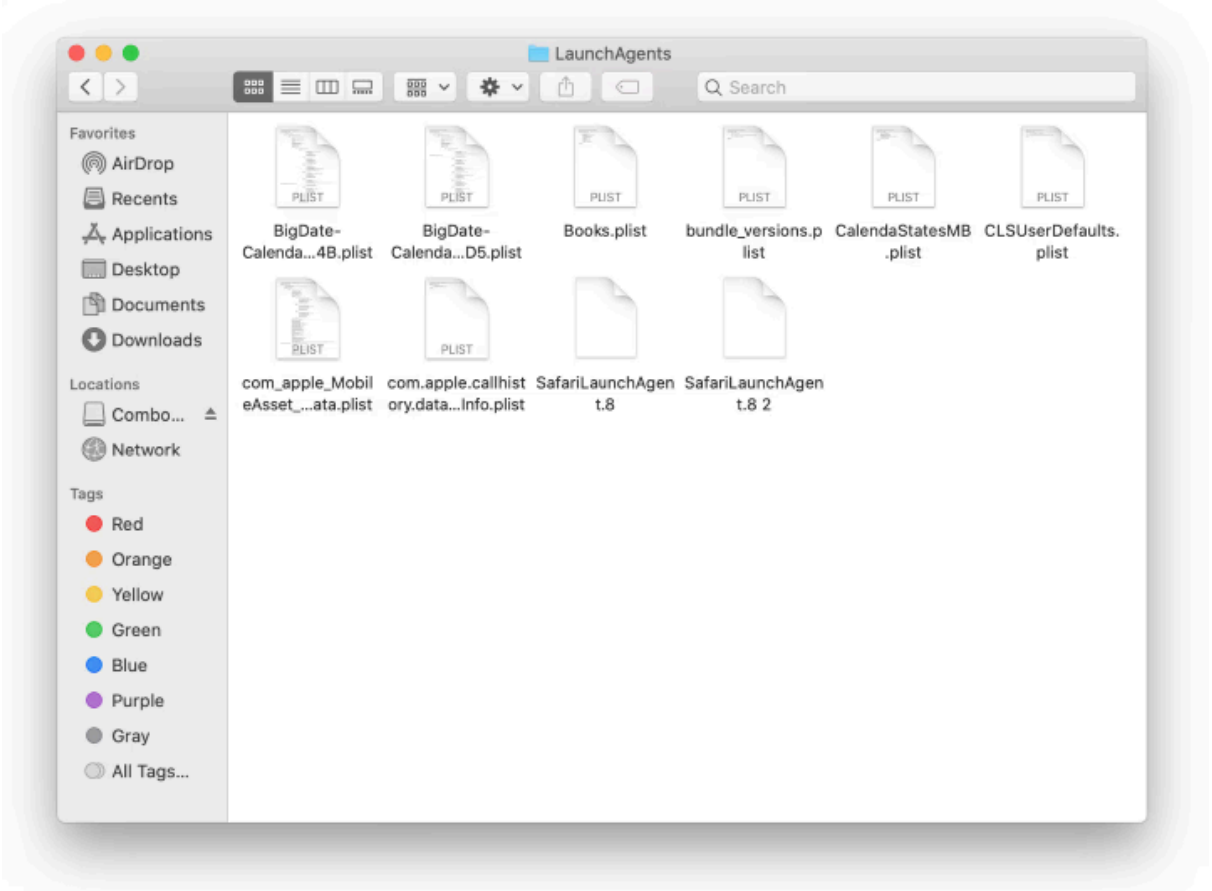
9. When the Application Support directory is opened, identify recently generated suspicious folders in it and send them to the Trash. A quick tip is to look for items whose names have nothing to do with Apple products or apps you knowingly installed. A few examples of known-malicious folder names are **com.AuraSearchDaemon**, **ProgressSite**, and **IdeaShared**.



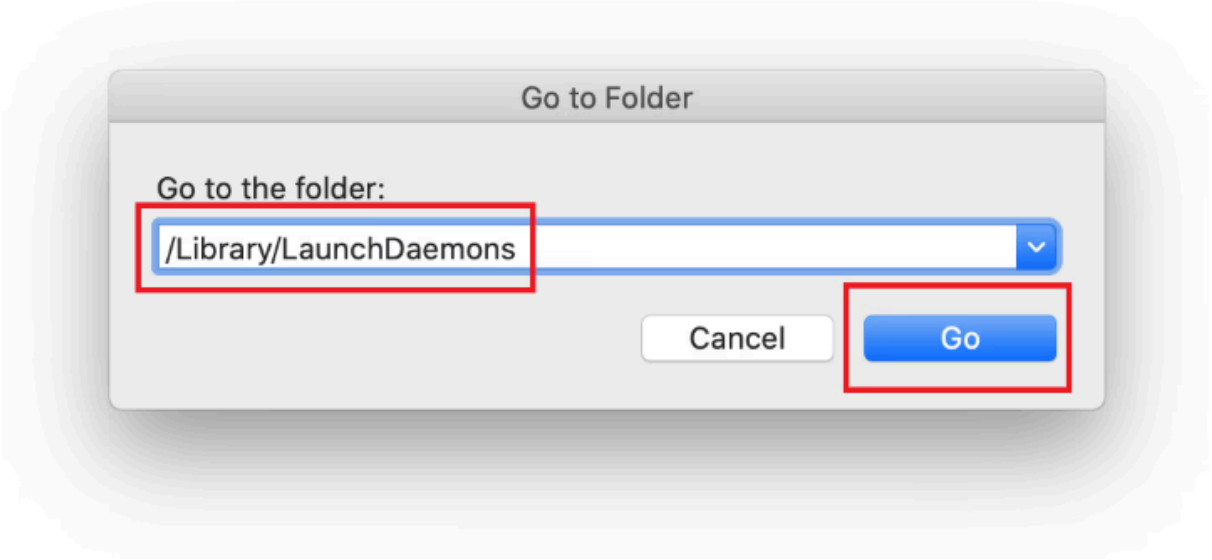
10. Enter **~/Library/LaunchAgents** string (don't forget to include the tilde character) in the **Go to Folder** search area.



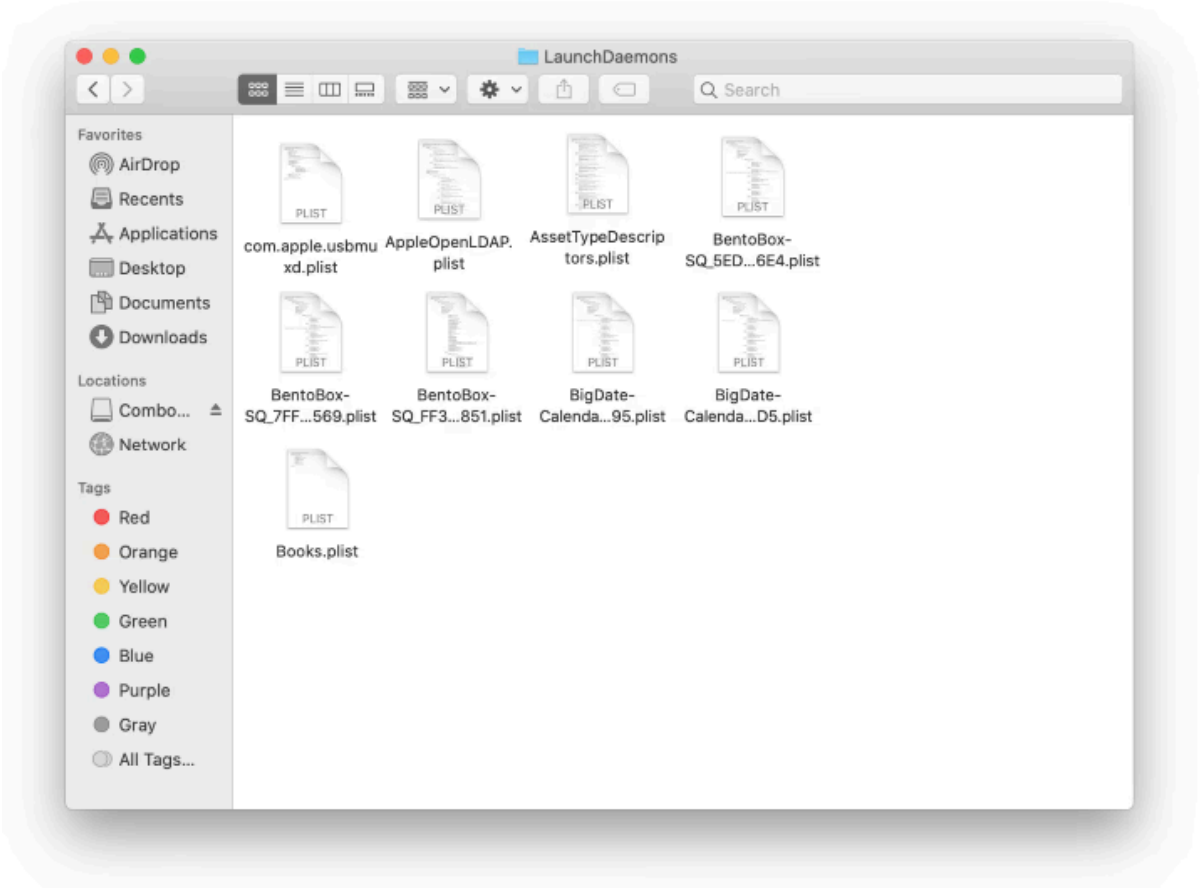
11. The system will display LaunchAgents residing in the current user's Home directory. Look for dodgy items related to guroshied.com popup virus (see logic highlighted in subsections above) and drag the suspects to the Trash.



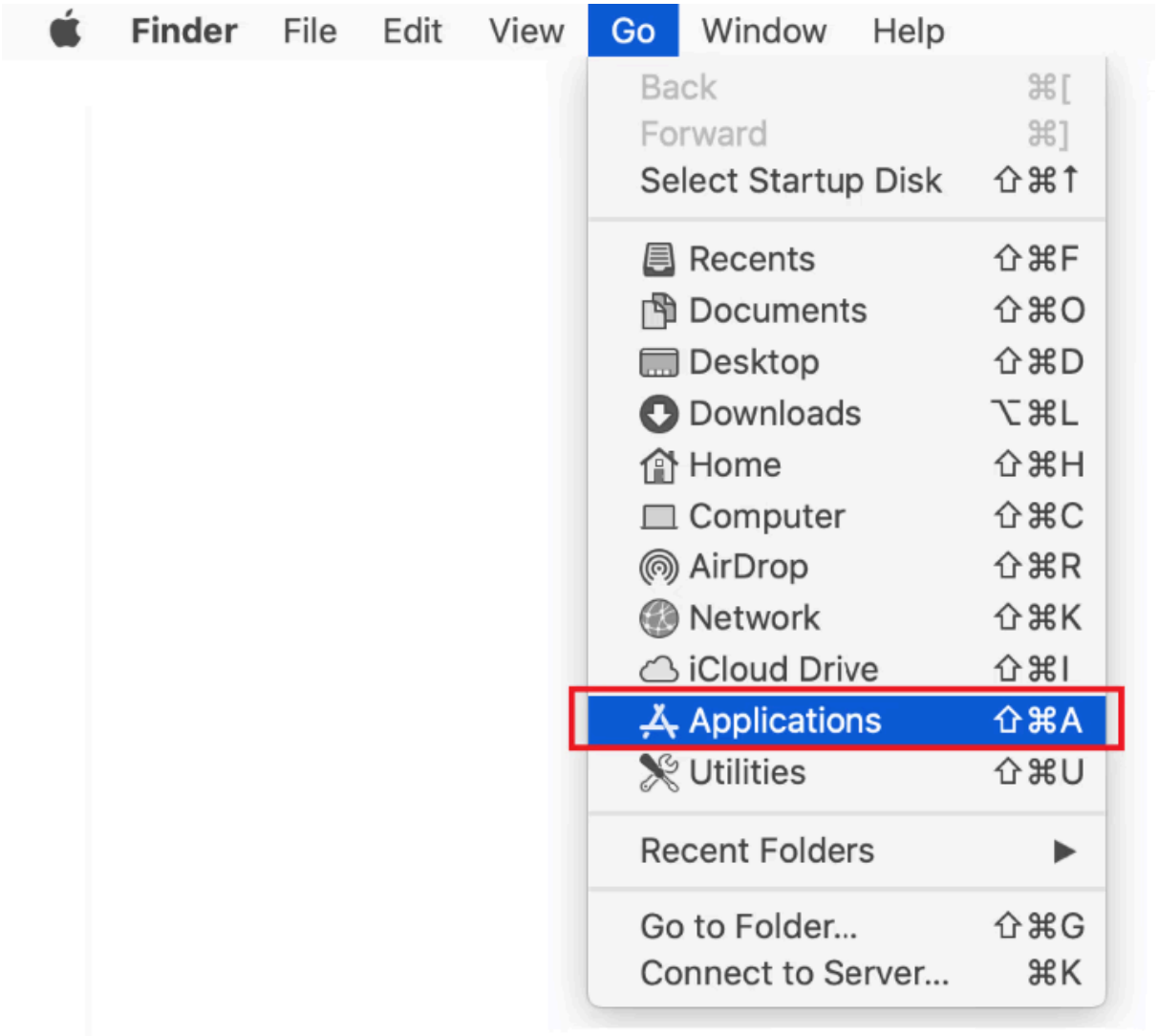
12. Type **/Library/LaunchDaemons** in the **Go to Folder** search field.



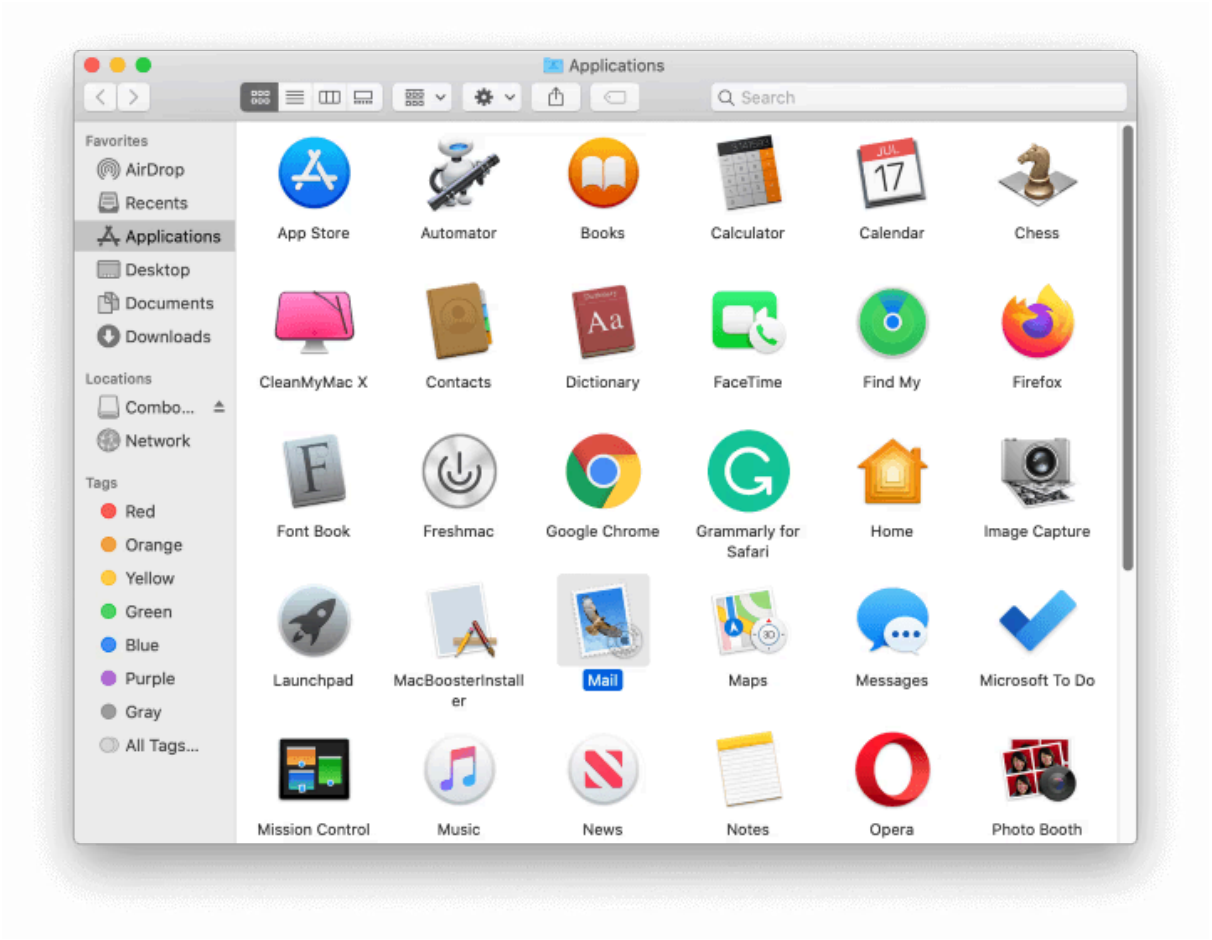
13. In the LaunchDaemons path, try to pinpoint the files the malware is using for persistence. Several examples of such items cropped by Mac infections are **com.pplauncher.plist**, **com.startup.plist**, and **com.ExpertModuleSearchDaemon.plist**. Delete the sketchy files immediately.



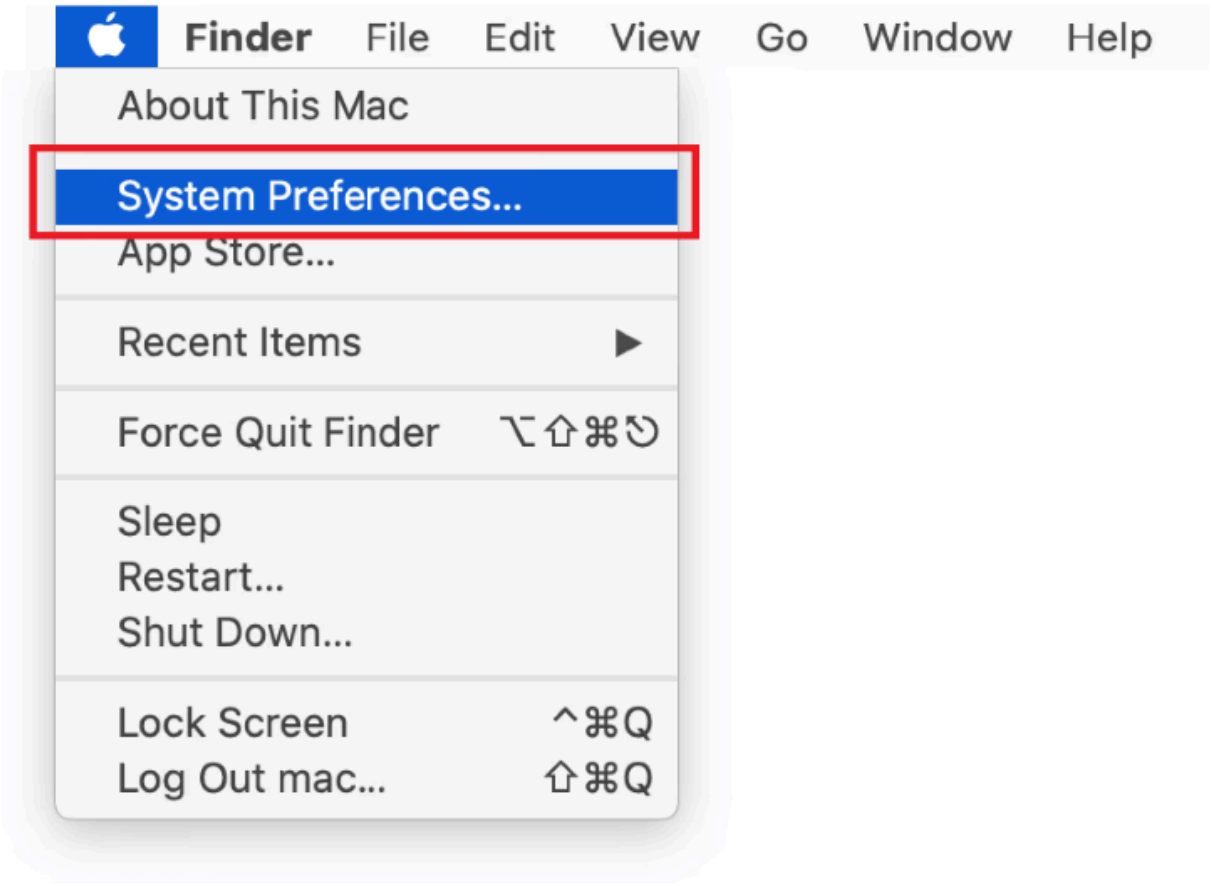
14. Click on the **Go** menu icon in your Mac's Finder and select **Applications** on the list.



15. Find the app that clearly doesn't belong there and move it to the Trash. If this action requires your admin password for confirmation, go ahead and enter it.

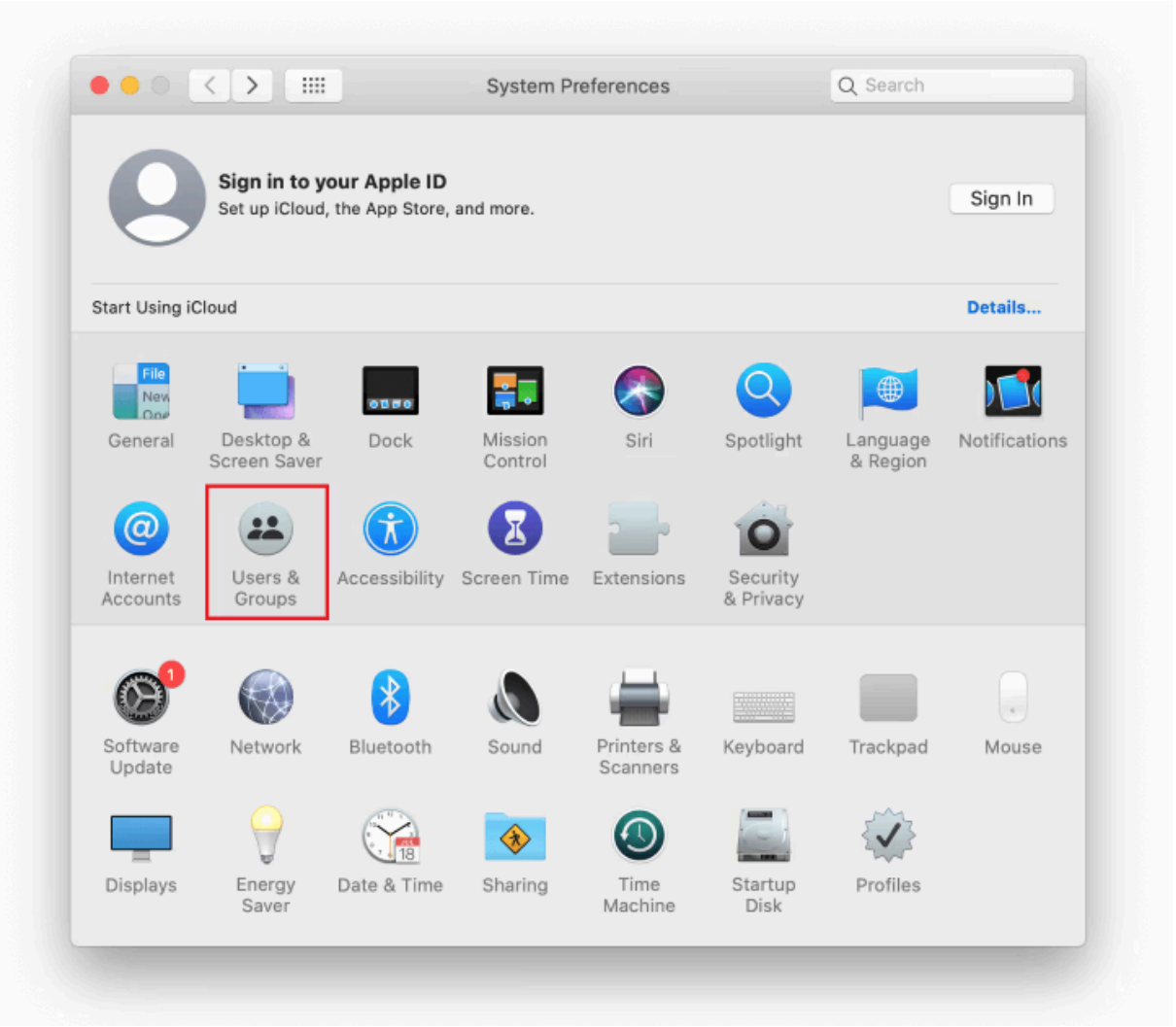

Applications
Search
Favorites
AirDrop
Recents
Applications
Desktop
Documents
Downloads
Locations
Combo...
Network
Tags
Red
Orange
Yellow
Green
Blue
Purple
Gray
All Tags...
App Store
Automator
Books
Calculator
Calendar
Chess
CleanMyMac X
Contacts
Dictionary
FaceTime
Find My
Firefox
Font Book
Freshmac
Google Chrome
Grammarly for Safari
Home
Image Capture
Launchpad
MacBoosterInstaller
Mail
Maps
Messages
Microsoft To Do
Mission Control
Music
News
Notes
Opera
Photo Booth

16. Expand the Apple menu and select **System Preferences**.



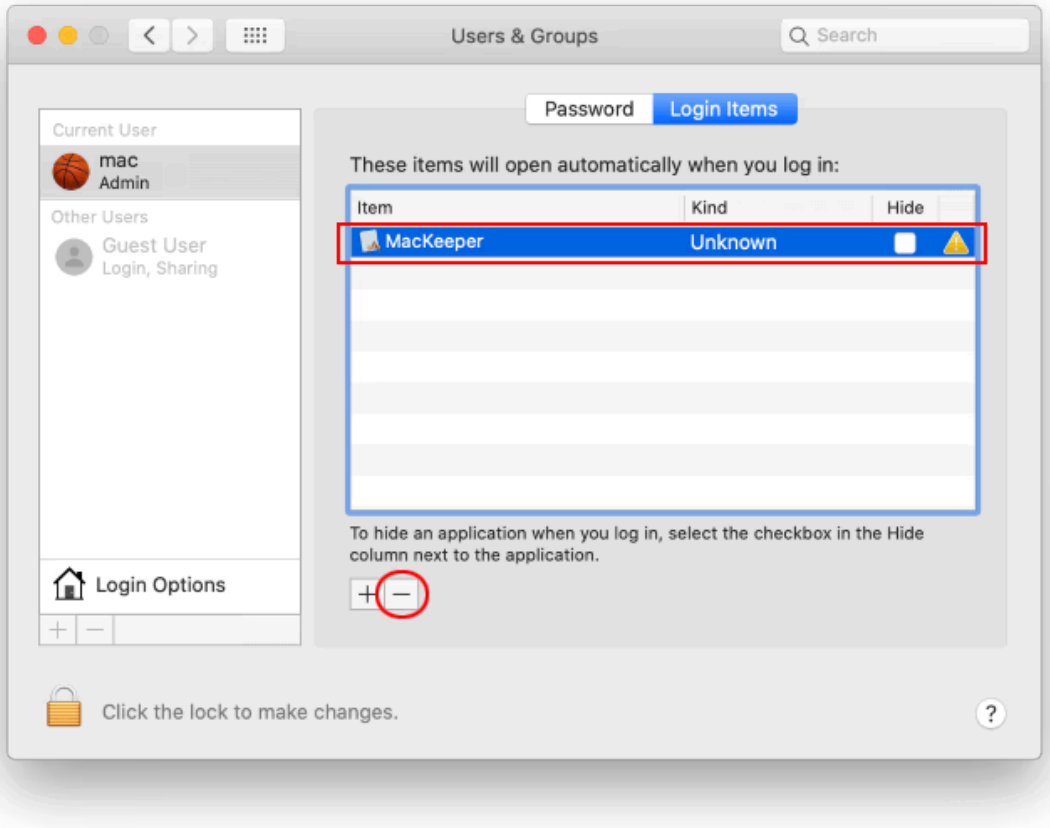

System Preferences
Search
Sign in to your Apple ID
Set up iCloud, the App Store, and more.
Sign In
Start Using iCloud
Details...
General
Desktop & Screen Saver
Dock
Mission Control
Siri
Spotlight
Language & Region
Notifications
Internet Accounts
Users & Groups
Accessibility
Screen Time
Extensions
Security & Privacy
Software Update
Network
Bluetooth
Sound
Printers & Scanners
Keyboard
Trackpad
Mouse
Displays
Energy Saver
Date & Time
Sharing
Time Machine
Startup Disk
Profiles

17. Proceed to **Users & Groups** and click on the **Login Items** tab.

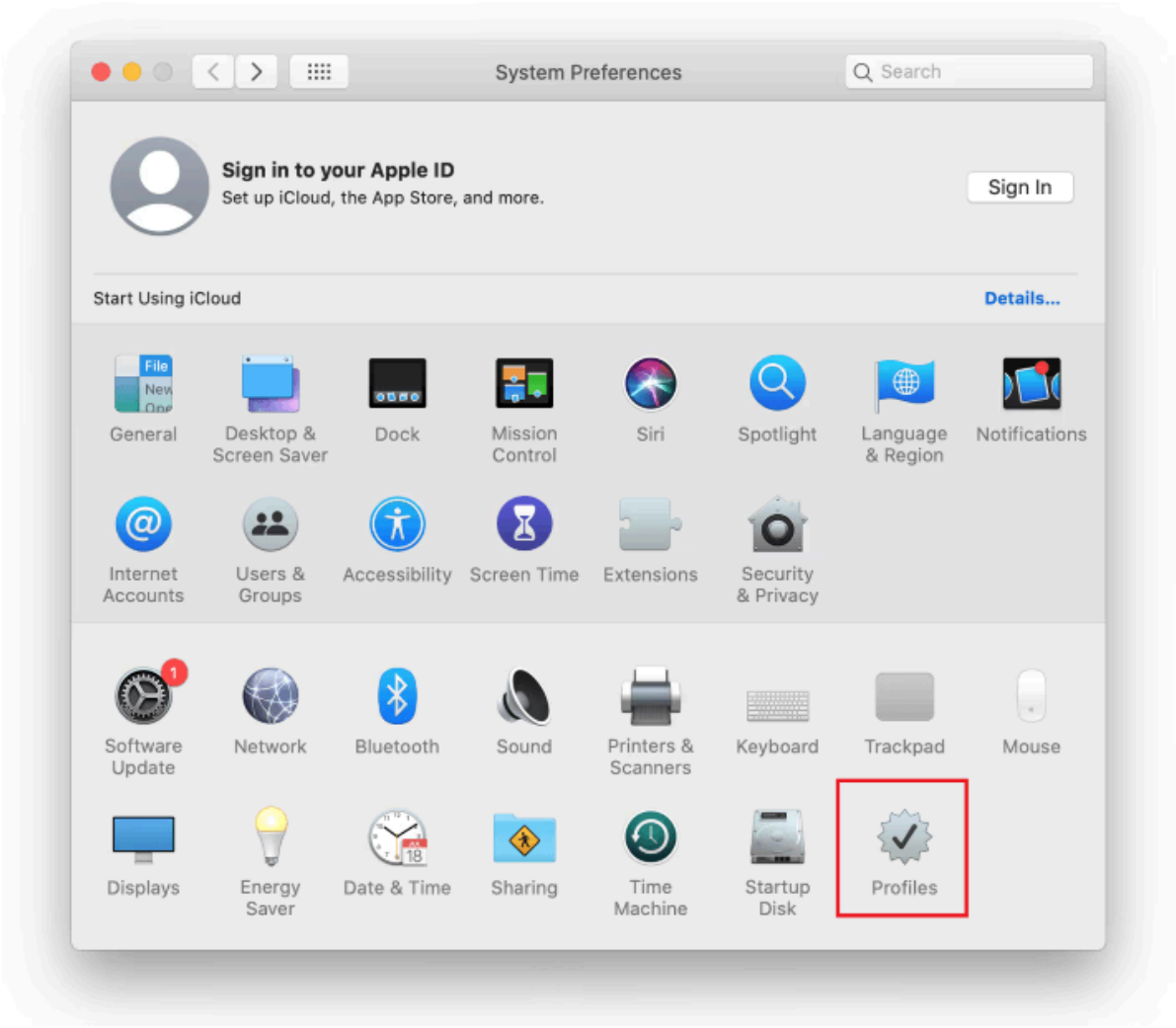


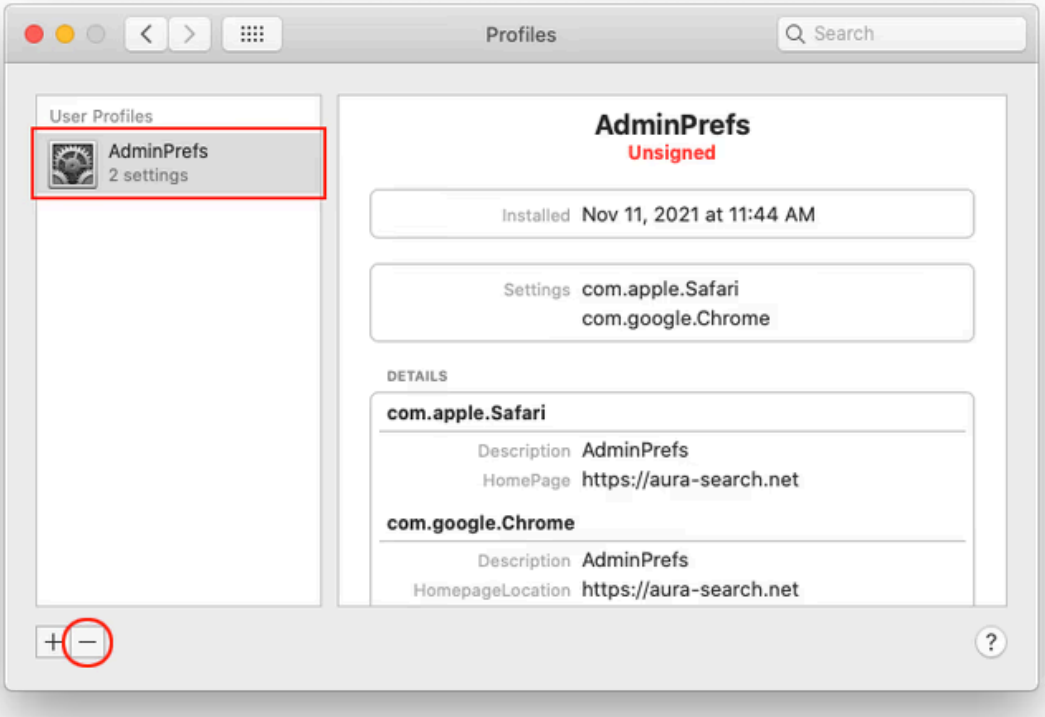
The system will display the list of items launched when the computer is starting up. Locate the potentially

unwanted app there and click on the “-” (minus) button.



18. Now select **Profiles** under System Preferences. Look for a malicious item in the left-hand sidebar. Several examples of configuration profiles created by Mac adware include **TechSignalSearch**, **MainSearchPlatform**, **AdminPrefs**, and **Safari Preferences**. Select the offending entity and click on the minus sign at the bottom to eliminate it.


System Preferences
Search
Sign in to your Apple ID
Set up iCloud, the App Store, and more.
Sign In
Start Using iCloud
Details...
General
Desktop & Screen Saver
Dock
Mission Control
Siri
Spotlight
Language & Region
Notifications
Internet Accounts
Users & Groups
Accessibility
Screen Time
Extensions
Security & Privacy
Software Update
Network
Bluetooth
Sound
Printers & Scanners
Keyboard
Trackpad
Mouse
Displays
Energy Saver
Date & Time
Sharing
Time Machine
Startup Disk
Profiles



> If your Mac has been infiltrated by adware, the infection will most likely continue to hold sway over your default web browser even after you remove the underlying application along with its components sprinkled around the system. Use the browser cleanup instructions below to address the remaining consequences of this attack.

To begin with, the web browser settings taken over by the Guroshied virus should be restored to their default values. Although this will clear most of your customizations, web surfing history, and all temporary data stored by websites, the malicious interference should be terminated likewise. The overview of the steps for completing this procedure is as follows:

1. **Remove guroshied.com virus popup in Safari**
2. **Remove Guroshied virus popup in Google Chrome**
3. **Remove guroshied.com popups in Mozilla Firefox**

Get rid of Guroshied virus using Combo Cleaner removal tool

The Mac maintenance and security app called **Combo Cleaner** is a one-stop tool to detect and remove Guroshied popup virus. This technique has substantial benefits over manual cleanup, because the utility gets hourly virus definition updates and can accurately spot even the newest Mac infections.

Furthermore, the automatic solution will find the core files of the malware deep down the system structure, which might otherwise be a challenge to locate. Here’s a walkthrough to sort out the Guroshied popup issue using Combo Cleaner:

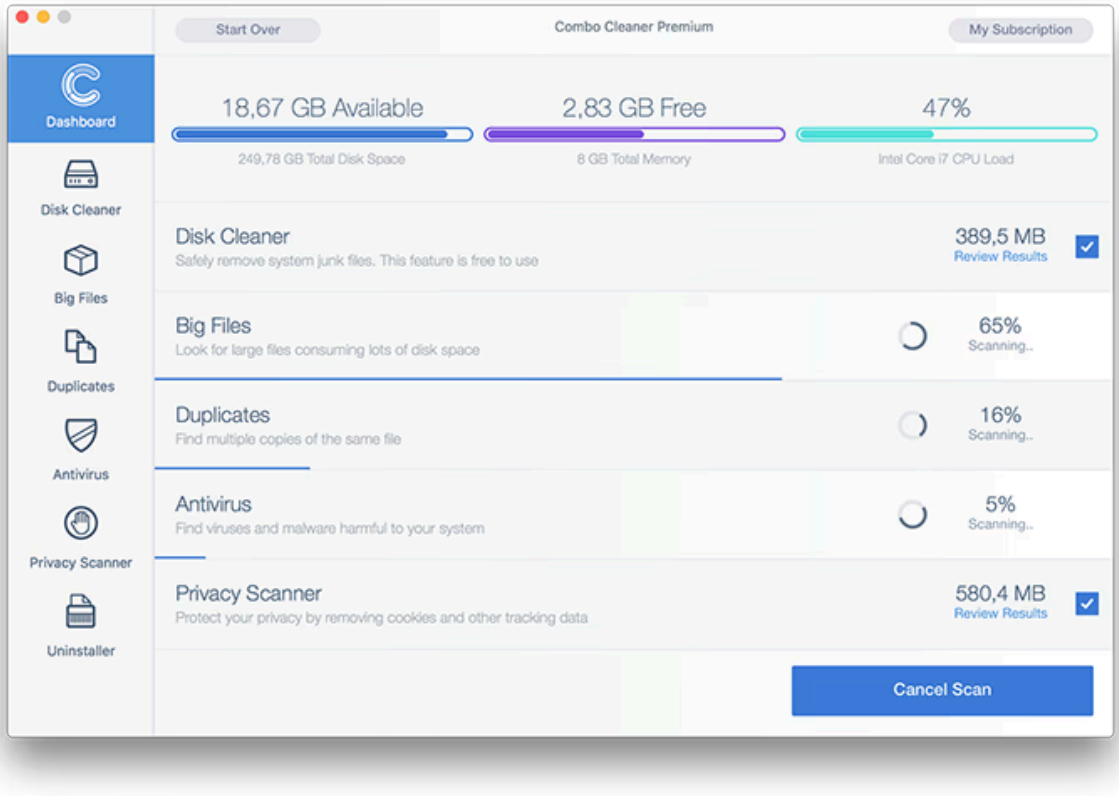
1. **Download Combo Cleaner installer**. When done, double-click the **combocleaner.dmg** file and follow the prompts to install the tool onto your Mac.

   Download Combo Cleaner

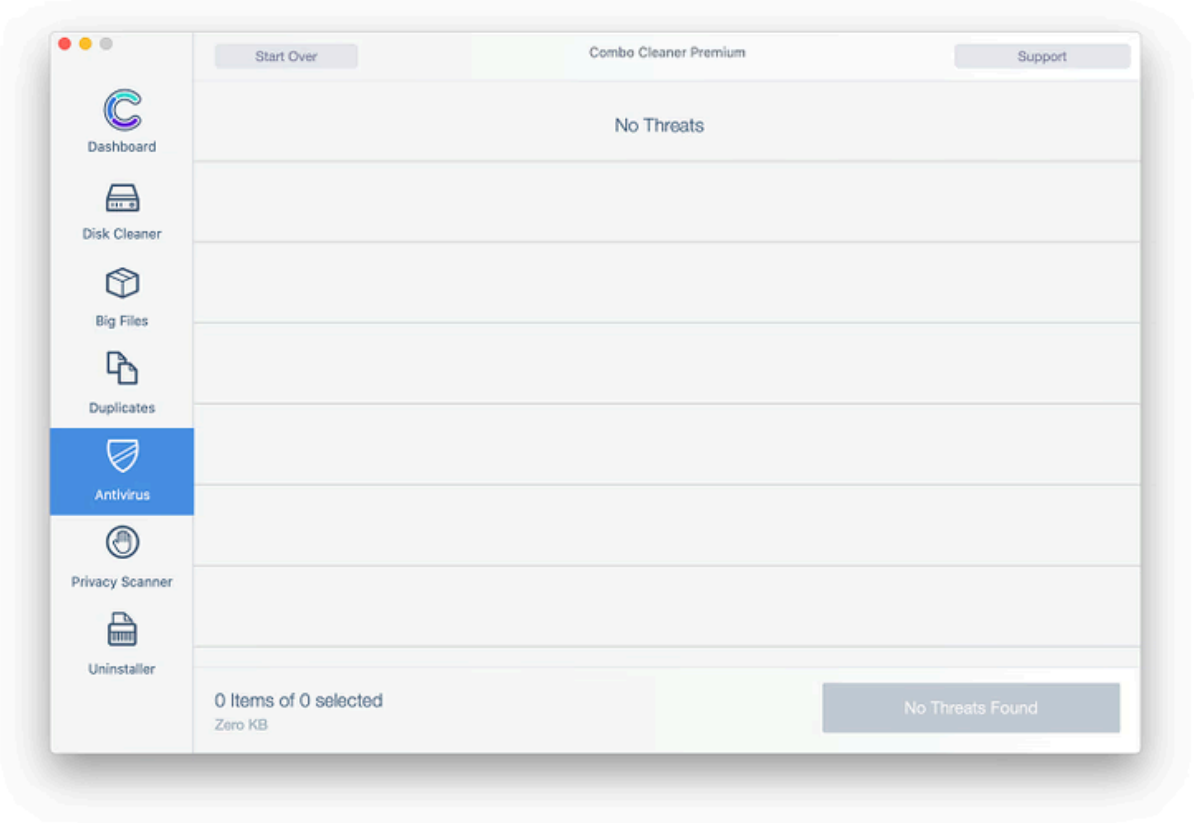
   By downloading any applications recommended on this website you agree to our Terms and Conditions and Privacy Policy. The free scanner checks whether your Mac is infected. To get rid of malware, you need to purchase the Premium version of Combo Cleaner.

2. Open the app from your Launchpad and let it run an update of the malware signature database to make sure it can identify the latest threats.

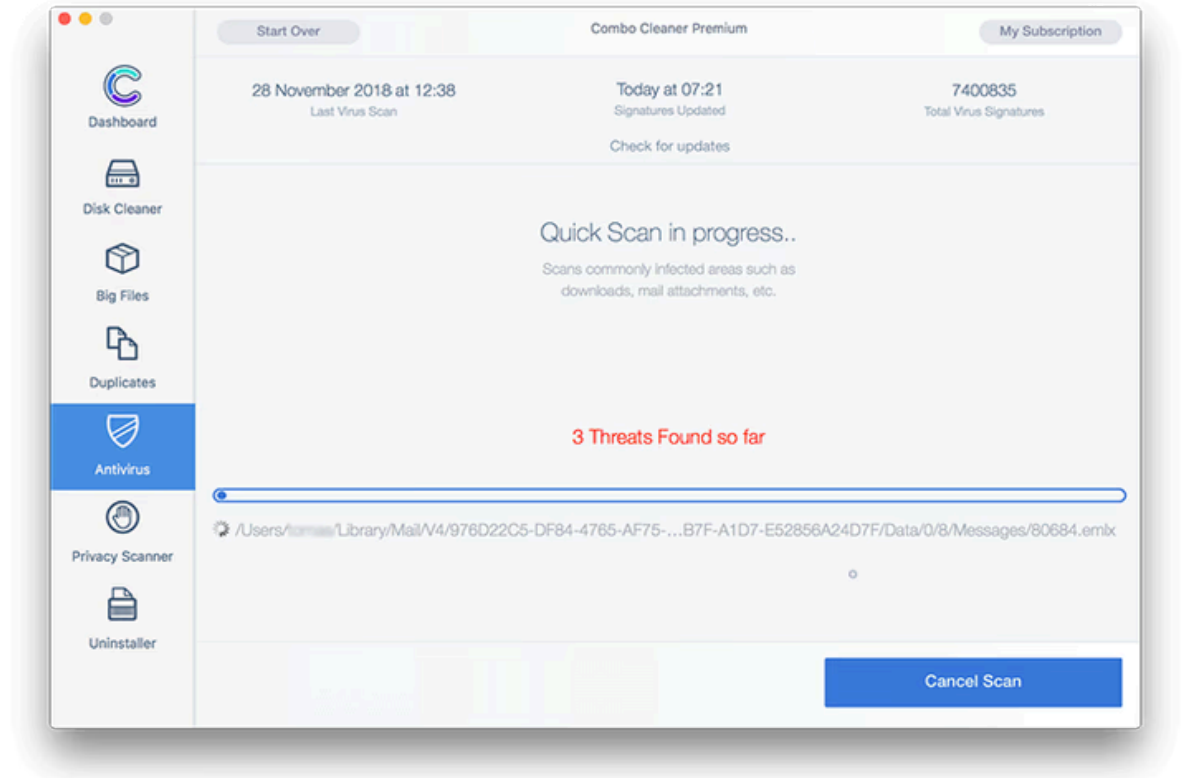
3. Click the **Start Combo Scan** button to check your Mac for malicious activity as well as performance issues.



4. Examine the scan results. If the report says “No Threats”, then you are on the right track with the manual cleaning and can safely proceed to tidy up the web browser that may continue to act up due to the after-effects of the malware attack (see instructions above).



5. In case Combo Cleaner has detected malicious code, click the **Remove Selected Items** button and have the utility remove Guroshied popup threat along with any other viruses, PUPs (potentially unwanted programs), or junk files that don't belong on your Mac.



6. Once you have made doubly sure that the malicious app is uninstalled, the browser-level troubleshooting might still be on your to-do list. If your preferred browser is affected, resort to the previous section of this tutorial to revert to hassle-free web surfing.
