

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] Malware Removal Guide for macOS \(MacBook & iMac\)](#)

Tha Sneak - March 20, 2025, 8:37 pm

? Malware Removal Guide for macOS (MacBook & iMac) ?

? Can Macs Get Malware? ?

Despite Apple's security measures, macOS is not immune to malware. Common threats include:

- ? Adware & Browser Hijackers – Redirects Safari/Chrome searches.
- ? Trojan Horses – Fake apps installing backdoors.
- ? Spyware & Keyloggers – Stealing data, keystrokes, and passwords.
- ? Cryptojackers – Secretly mining cryptocurrency, causing overheating.
- ? Ransomware – Encrypting files & demanding payment.

? Tip: If your Mac runs slow, overheats, has pop-ups, or redirects searches, it may be infected.

? Step 1: Remove Suspicious Apps

Some malware disguises itself as legitimate applications.

? Delete Malicious Apps

- 1 Open Finder -> Applications.
- 2 Look for unknown, suspicious, or recently installed apps.
- 3 Drag them to the Trash, then empty it.
- 4 Restart your Mac.

? Tip: If the app won't delete, boot into Safe Mode and try again.

? Step 2: Remove Malware from Login Items

Malware often starts automatically when you log in.

? Check Login Items

- 1 Open System Settings -> General -> Login Items.
- 2 Look for unwanted programs.
- 3 Select them and click the "-" (minus) button to remove them.

? Tip: If you see something suspicious, Google its name to verify if it's malware.

? Step 3: Remove Malicious Browser Extensions

? Safari

- 1 Open Safari -> Click Safari (top-left) -> Settings.
- 2 Go to the Extensions tab.
- 3 Remove any suspicious extensions.

? Chrome

- 1 Open Chrome -> Click ? (top-right menu) -> Extensions.
- 2 Look for unknown extensions and click Remove.

? Firefox

- 1 Open Firefox -> Click ? (top-right menu) -> Add-ons & Extensions.
- 2 Remove anything unfamiliar.

? Tip: If malware persists, reset the browser to default settings.

? Step 4: Remove Malicious Configuration Profiles

Some malware installs configuration profiles to modify system settings.

? Check for Malicious Profiles

- 1 Open System Settings -> Privacy & Security -> Profiles.
- 2 If you see an unknown profile, select it and click Remove (-).
- 3 Restart your Mac.

? Tip: Profiles are often used for VPNs, ad blockers, or remote management malware.

? Step 5: Check Activity Monitor for Suspicious Processes

If malware is running in the background, it may show up in Activity Monitor.

? Kill Malicious Processes

- 1 Open Finder -> Applications -> Utilities -> Activity Monitor.
- 2 Look for high CPU or memory usage from unknown processes.
- 3 Select the process and click Quit (?) -> Force Quit.

? Tip: If unsure, Google the process name to check if it's safe.

? Step 6: Remove Malware-Related Files

Some malware hides in system directories.

? Delete Malware Files from ~/Library

- 1 Open Finder -> Click Go -> Go to Folder.
- 2 Enter the following paths and check for unknown files:

Code ~/Library/Application Support

Code ~/Library/LaunchAgents

Code ~/Library/LaunchDaemons

Code ~/Library/Preferences

Code ~/Library/Caches

- 3 Delete anything suspicious.

? Tip: Be careful not to delete system files.

? Step 7: Scan for Malware with Malwarebytes

? Download Malwarebytes for Mac

1 Go to [Malwarebytes Official Site](https://www.malwarebytes.com).

2 Download and install Malwarebytes for Mac.

3 Run a full system scan.

4 Remove any detected threats.

? Tip: Use Malwarebytes Free for manual scans or Premium for real-time protection.

? Step 8: Reset Your Mac's Hosts File (If Internet is Hijacked)

Malware can modify the hosts file to redirect your internet traffic.

? Reset the Hosts File

1 Open Terminal.

2 Enter the command:

Code `sudo nano /etc/hosts`

3 If you see unknown entries, delete them.

4 Press CTRL + X, then Y, and hit Enter to save changes.

5 Restart your Mac.

? Tip: If websites still redirect, reset Wi-Fi settings.

? Step 9: Keep macOS Updated

? Update macOS & Security Patches

1 Open System Settings -> General -> Software Update.

2 If an update is available, click Download & Install.

? Tip: Updates patch security vulnerabilities used by malware.

? Step 10: Factory Reset (Last Resort)

If malware persists, consider a factory reset.

? Erase & Reinstall macOS

1 Boot into macOS Recovery (Hold Command + R while restarting).

2 Select Disk Utility -> Erase Mac.

3 Reinstall macOS from macOS Utilities.

? Tip: Backup important files before resetting!

? Conclusion

By following this guide, you can effectively remove malware from macOS.

- ? Uninstall suspicious apps.
- ? Remove malicious browser extensions & profiles.
- ? Use Malwarebytes to scan & remove threats.
- ? Reset network settings if internet is hijacked.
- ? Factory reset as a last resort.

? Tip: To prevent future infections, avoid downloading pirated software and use ad blockers & security tools.

Pr0m3th3us - March 20, 2025, 8:59 pm

Gosh i wish windows was this simple XD

AnnaCred - January 30, 2026, 10:43 pm

(Mar 20, 2025 08:37 PM)Tha Sneak Wrote: [\[CITE\]](#)

? Malware Removal Guide for macOS (MacBook & iMac) ?

? Can Macs Get Malware? ?

Despite Apple's security measures, macOS is not immune to malware.
Common threats include:

- ? Adware & Browser Hijackers – Redirects Safari/Chrome searches.
- ? Trojan Horses – Fake apps installing backdoors.
- ? Spyware & Keyloggers – Stealing data, keystrokes, and passwords.
- ? Cryptojackers – Secretly mining cryptocurrency, causing overheating.
- ? Ransomware – Encrypting files & demanding payment.

? Tip: If your Mac runs slow, overheats, has pop-ups, or redirects searches, it may be infected.

? Step 1: Remove Suspicious Apps

Some malware disguises itself as legitimate applications.

? Delete Malicious Apps

- 1 Open Finder -> Applications.
- 2 Look for unknown, suspicious, or recently installed apps.
- 3 Drag them to the Trash, then empty it.
- 4 Restart your Mac.

? Tip: If the app won't delete, boot into Safe Mode and try again.

? Step 2: Remove Malware from Login Items

Malware often starts automatically when you log in.

? Check Login Items

- 1 Open System Settings -> General -> Login Items.
- 2 Look for unwanted programs.
- 3 Select them and click the "-" (minus) button to remove them.

? Tip: If you see something suspicious, Google its name to verify if it's malware.

? Step 3: Remove Malicious Browser Extensions

? Safari

- 1 Open Safari -> Click Safari (top-left) -> Settings.
- 2 Go to the Extensions tab.
- 3 Remove any suspicious extensions.

? Chrome

- 1 Open Chrome -> Click ? (top-right menu) -> Extensions.
- 2 Look for unknown extensions and click Remove.

? Firefox

- 1 Open Firefox -> Click ? (top-right menu) -> Add-ons & Extensions.
- 2 Remove anything unfamiliar.

? Tip: If malware persists, reset the browser to default settings.

? Step 4: Remove Malicious Configuration Profiles

Some malware installs configuration profiles to modify system settings.

? Check for Malicious Profiles

- 1 Open System Settings -> Privacy & Security -> Profiles.
- 2 If you see an unknown profile, select it and click Remove (-).
- 3 Restart your Mac.

? Tip: Profiles are often used for VPNs, ad blockers, or remote management malware.

? Step 5: Check Activity Monitor for Suspicious Processes

If malware is running in the background, it may show up in Activity Monitor.

? Kill Malicious Processes

- 1 Open Finder -> Applications -> Utilities -> Activity Monitor.
- 2 Look for high CPU or memory usage from unknown processes.
- 3 Select the process and click Quit (?) -> Force Quit.

? Tip: If unsure, Google the process name to check if it's safe.

? Step 6: Remove Malware-Related Files

Some malware hides in system directories.

? Delete Malware Files from ~/Library

- 1 Open Finder -> Click Go -> Go to Folder.
- 2 Enter the following paths and check for unknown files:

Code ~/Library/Application Support
Code ~/Library/LaunchAgents
Code ~/Library/LaunchDaemons
Code ~/Library/Preferences
Code ~/Library/Caches
3 Delete anything suspicious.

? Tip: Be careful not to delete system files.

? Step 7: Scan for Malware with Malwarebytes

? Download Malwarebytes for Mac

- 1 Go to [Malwarebytes Official Site](#).
- 2 Download and install Malwarebytes for Mac.
- 3 Run a full system scan.
- 4 Remove any detected threats.

? Tip: Use Malwarebytes Free for manual scans or Premium for real-time protection.

? Step 8: Reset Your Mac's Hosts File (If Internet is Hijacked)

Malware can modify the hosts file to redirect your internet traffic.

? Reset the Hosts File

- 1 Open Terminal.
- 2 Enter the command:
Code sudo nano /etc/hosts
- 3 If you see unknown entries, delete them.
- 4 Press CTRL + X, then Y, and hit Enter to save changes.
- 5 Restart your Mac.

? Tip: If websites still redirect, reset Wi-Fi settings.

? Step 9: Keep macOS Updated

? Update macOS & Security Patches

- 1 Open System Settings -> General -> Software Update.
- 2 If an update is available, click Download & Install.

? Tip: Updates patch security vulnerabilities used by malware.

? Step 10: Factory Reset (Last Resort)

If malware persists, consider a factory reset.

? Erase & Reinstall macOS

- 1 Boot into macOS Recovery (Hold Command + R while restarting).
- 2 Select Disk Utility -> Erase Mac.

3 Reinstall macOS from macOS Utilities.

? Tip: Backup important files before resetting!

? Conclusion

By following this guide, you can effectively remove malware from macOS.

? Uninstall suspicious apps.

? Remove malicious browser extensions & profiles.

? Use Malwarebytes to scan & remove threats.

? Reset network settings if internet is hijacked.

? Factory reset as a last resort.

? Tip: To prevent future infections, avoid downloading pirated software and use ad blockers & security tools.

Thanks!

habeotron - March 24, 2026, 6:25 pm

thank you. high value of information