

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] Malware Removal Guide for Linux](#)

Tha Sneak - March 20, 2025, 11:30 pm

? Malware Removal Guide for Linux ?

? Can Linux Get Malware?

While Linux is more secure by design than other operating systems, it is not immune to malware. Threats include:

- ? Rootkits
- ? Trojans disguised as .sh scripts or packages
- ? Crypto miners
- ? Malicious repositories
- ? Backdoored software

? Tip: Malware on Linux often targets servers, misconfigured systems, or users running as root unnecessarily.

? Step 1: Check for Suspicious Processes

Use terminal commands to view running processes:

```
Code ps aux --sort=-%cpu  
top  
htop
```

? Look for unknown processes using excessive CPU, memory, or network.

? Tip: Install htop using your package manager for an interactive view:

```
Code sudo apt install htop
```

? Step 2: Scan with ClamAV or RKHunter

Install and run open-source antivirus tools:

? ClamAV – Virus scanner

```
Code sudo apt update  
sudo apt install clamav  
sudo freshclam
```

```
sudo clamscan -r /
```

? RKHunter – Rootkit scanner

Code `sudo apt install rkhunter`
`sudo rkhunter --update`
`sudo rkhunter --check`
? Tip: For CentOS/RHEL/Fedora, use yum or dnf instead of apt.

? Step 3: Check Cron Jobs & Startup Scripts

Check for suspicious scheduled tasks or auto-starting malware:

Code `crontab -l`
`sudo ls -la /etc/cron*`
`sudo ls -la ~/.config/autostart/`
? Delete unknown entries carefully.

? Tip: Malicious cron jobs may download payloads or run miners silently.

? Step 4: Review Installed Packages

Check for unfamiliar or malicious packages:

Code `dpkg -l` # For Debian/Ubuntu
`rpm -qa` # For RedHat/CentOS
? Remove suspicious packages:
Code `sudo apt remove [package]`
? Tip: Always install software from trusted repositories. Avoid unknown PPAs or external .deb/.rpm files.

? Step 5: Monitor Network Activity

Use tools to spot suspicious network connections:

Code `netstat -tulnp`
`ss -tuln`
`lsof -i`
? Look for unfamiliar IPs or services bound to unusual ports.

? Tip: Install nethogs or iftop to monitor per-process bandwidth usage.

? Step 6: Analyze Bash History & Aliases

Check for malware launched through terminal:

Code `cat ~/.bash_history`
`alias`
? Look for:

- Scripts you didn't run
- Hidden curl/wget commands
- Aliases masking common commands (e.g., ls, cd, sudo)

? Tip: Some malware modifies .bashrc or .profile — inspect them if unsure.

? Step 7: Scan for Malicious Files

Run a full disk scan with ClamAV:

Code `sudo clamscan -r --bell -i /`

This command will:

- Scan recursively (-r)
- Ring the bell on detection (--bell)
- Show infected files only (-i)

? Tip: You can scan just your home folder for faster results:

Code `clamscan -r ~/`

? Step 8: Clean or Reinstall Affected Systems

If your system is heavily infected:

- ? Backup important files.
- ? Wipe and reinstall a clean Linux distro.
- ? Avoid restoring binaries or config files unless verified safe.

? Tip: Use checksum tools (sha256sum) to verify ISO integrity before reinstalling.

? Tips to Stay Protected on Linux

- ? Avoid logging in as root for regular tasks.
- ? Use a firewall (e.g., ufw) to block unnecessary ports.
- ? Keep your system updated:
Code `sudo apt update && sudo apt upgrade`
- ? Don't install software from untrusted sources.
- ? Monitor system logs with journalctl or /var/log/syslog.

? Linux is secure, but only if you practice good hygiene! ?

Bastille - March 21, 2025, 1:54 am

Nice check list, thanks for the thread

+1 for Linux hardening, I think we can rely on CIS check lists <https://www.cisecurity.org/benchmark>

Pr0m3th3us - March 21, 2025, 3:45 am

Great thread as usual, it seems you know how to remove malware from anything.

