

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] How to Detect and Remove a Rootkit](#)

Tha Sneak - February 14, 2025, 7:26 pm

How to Detect and Remove a Rootkit

What is a Rootkit?

A rootkit is a type of malicious software that hides itself within the operating system to maintain persistence and avoid detection. It can:

- Hide files, processes, and registry keys.

- Gain administrative privileges (system-level access).

- Bypass security measures, including antivirus software.

- Remotely control your system without detection.

Step 1: Signs of a Rootkit Infection

Common symptoms of a rootkit include:

- Unexpected system crashes or BSODs (Blue Screen of Death).

- High CPU or disk usage without explanation.

- Antivirus or security software suddenly disabled.

- Strange network activity or high outbound traffic.

- Unknown system processes that cannot be terminated.

- Unauthorized registry modifications.

Step 2: Detecting a Rootkit

Use the following methods to check for a rootkit:

1. Run Windows System File Checker (SFC) and DISM
- Open Command Prompt as Administrator.

Run the following command:

Code `sfc /scannow`

If issues are found but cannot be fixed, run:
Code DISM /Online /Cleanup-Image /RestoreHealth
Restart your computer.

2. Scan with Rootkit Detection Tools

Use specialized rootkit scanners: [Malwarebytes Anti-Rootkit](#)

[Kaspersky TDSSKiller](#)

[McAfee Rootkit Remover](#)

[Sophos Anti-Rootkit](#)

3. Use GMER for Advanced Rootkit Detection

Download GMER from: <https://www.gmer.net/>

Run GMER and select "Scan."

Look for suspicious hidden processes or registry modifications.

Do not delete files unless you are sure they are malicious.

4. Check for Hidden Network Activity

Open Command Prompt as Administrator.

Run:

Code netstat -ano | findstr LISTENING

Look for unknown network connections.

Compare them against known system processes.

Step 3: Removing a Rootkit

Method 1: Using Rootkit Removal Tools

Boot into Safe Mode by pressing F8 during startup.

Run Malwarebytes Anti-Rootkit or Kaspersky TDSSKiller.

Follow the on-screen instructions to remove threats.

Restart your PC.

Method 2: Removing a Rootkit with FRST (Farbar Recovery Scan Tool)

Download FRST from: [BleepingComputer](#).

Boot into Windows Recovery Mode (WinRE).

Open Command Prompt and run FRST.

Perform a scan and check the `FRST.txt` log for unknown drivers or hidden services.

Create a Fixlist.txt to delete suspicious entries and click "Fix."

Restart your computer.

Method 3: Manually Removing a Rootkit

If scanners fail, you may need to manually remove the rootkit: Identify suspicious drivers by running:

Code `sc query type= driver`

Locate and delete suspicious files in `C:\Windows\System32\drivers\`.

Modify the registry (if necessary) by running:

Code `regedit`

Navigate to:

Code `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`

Look for suspicious entries and delete them.

Restart your PC.

Tha Sneak - *March 1, 2025, 8:36 pm*

Please do NOT reply to this thread in case information needs to be added or edited.

If you have a questions about the contents of the thread or other tutorials please go to this thread and post your question in this thread: <https://hackforums.net/showthread.php?tid=6293473>

Thanks,

Tha Sneak