I performed a host-based forensic validation covering persistence mechanisms, execution paths, system integrity, and security logs. No residual artifacts or unauthorized persistence mechanisms were identified.

Final Validation Checklist

The following forensic validation steps were performed to confirm that no persistence mechanisms or unauthorized artifacts remained on the system after remediation.

Persistence Verification

- Re-reviewed **Task Scheduler** (root and all subfolders)
  - Confirmed no remaining tasks invoking cmd.exe, powershell.exe, WMI, or script-based execution
- Verified startup folders were clean:
  - shell:startup
  - shell:common startup
- Inspected registry Run keys:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run

Script & Execution Review

- Reviewed **PowerShell Operational logs** (Event ID 4104)
- Confirmed no recent obfuscated or encoded PowerShell execution
- Searched for unexpected script files (.ps1, .vbs, .js, .hta) in user and system directories

Services & Drivers

- Audited Windows services for:
  - Unknown vendors
  - Non-standard execution paths (AppData, Temp)
- Reviewed loaded drivers using driverquery /v
  - Confirmed only signed drivers from known vendors

Event Log Correlation

- Reviewed **Security** logs for abnormal logon activity or scheduled task creation
- Reviewed **System** logs for power-related events
  - Confirmed AC power connection no longer triggered program execution

System Integrity & Anti-Malware

- Verified Windows integrity:
  - sfc /scannow
  - DISM /Online /Cleanup-Image /RestoreHealth
- Completed Microsoft Defender **Offline Scan** with no detections

Validation Outcome:
No residual persistence mechanisms or unauthorized activity were identified. The system is considered clean and suitable for personal daily use.