





# /Unregmp2.exe

☆ Star

7,060

Execute

Microsoft Windows Media Player Setup Utility

**Paths:**

C:\Windows\System32\unregmp2.exe  
C:\Windows\SysWOW64\unregmp2.exe

**Resources:**

- <https://twitter.com/notwhickey/status/1466588365336293385>

**Acknowledgements:**

- Wade Hickey ([@notwhickey](#))

**Detections:**

- Sigma: [proc\\_creation\\_win\\_lolbin\\_unregmp2.yml](#)
- IOC: Low-prevalence binaries, with filename 'wmpnscfg.exe', spawned as child-processes of `unregmp2.exe /HideWMP`

## Execute

Allows an attacker to copy a target binary to a controlled directory and modify the 'ProgramW6432' environment variable to point to that controlled directory, then execute 'unregmp2.exe' with argument '/HideWMP' which will spawn a process at the hijacked path '%ProgramW6432%\wmpnscfg.exe'.

```
rmdir %temp%\lolbin /s /q 2>nul & mkdir "%temp%\lolbin\Windows Media Player" & copy
C:\Windows\System32\calc.exe "%temp%\lolbin\Windows Media Player\wmpnscfg.exe" >nul && cmd /V /C "set
"ProgramW6432=%temp%\lolbin" && unregmp2.exe /HideWMP"
```

**Use case:** Proxy execution of binary  
**Privileges required:** User  
**Operating systems:** Windows 10  
**ATT&CK® technique:** [T1202: Indirect Command Execution](#)