



/AgentExecutor.exe ☆ Star 7,060

Execute

Intune Management Extension included on Intune Managed Devices

Paths:

C:\Program Files (x86)\Microsoft Intune Management Extension\AgentExecutor.exe

Acknowledgements:

- Eleftherios Panos ([@liferispan](#))

Detections:

- Sigma: [proc_creation_win_lolbin_agentexecutor.yml](#)
- Sigma: [proc_creation_win_lolbin_agentexecutor_susp_usage.yml](#)

Execute

- Spawns powershell.exe and executes a provided powershell script with ExecutionPolicy Bypass argument

```
AgentExecutor.exe -powershell "c:\temp\malicious.ps1" "c:\temp\test.log" "c:\temp\test1.log"
"c:\temp\test2.log" 60000 "C:\Windows\SysWOW64\WindowsPowerShell\v1.0" 0 1
```

Use case: Execute unsigned powershell scripts
Privileges required: User
Operating systems: Windows 10
ATT&CK® technique: [T1218: System Binary Proxy Execution](#)

- If we place a binary named powershell.exe in the path c:\temp, agentexecutor.exe will execute it successfully

```
AgentExecutor.exe -powershell "c:\temp\malicious.ps1" "c:\temp\test.log" "c:\temp\test1.log"
"c:\temp\test2.log" 60000 "C:\temp\" 0 1
```

Use case: Execute a provided EXE
Privileges required: User
Operating systems: Windows 10
ATT&CK® technique: [T1218: System Binary Proxy Execution](#)