

# .. /Runonce.exe

Execute

Executes a Run Once Task that has been configured in the registry

## Paths:

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

## Resources:

- <https://twitter.com/pabraeken/status/990717080805789697>
- <https://cmatskas.com/configure-a-runonce-task-on-windows/>

## Acknowledgements:

- Pierre-Alexandre Braeken (@[pabraeken](#))

## Detections:

- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/registry/registry\\_event/registry\\_event\\_runonce\\_persistence.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/registry/registry_event/registry_event_runonce_persistence.yml)
- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process\\_creation/proc\\_creation\\_win\\_runonce\\_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_runonce_execution.yml)
- Elastic: [https://github.com/elastic/detection-rules/blob/2926e98c5d998706ef7e248a63fb0367c841f685/rules/windows/persistence\\_run\\_key\\_and\\_startup\\_broad.toml](https://github.com/elastic/detection-rules/blob/2926e98c5d998706ef7e248a63fb0367c841f685/rules/windows/persistence_run_key_and_startup_broad.toml)
- IOC: Registry key add - HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\YOURKEY

## Execute

Executes a Run Once Task that has been configured in the registry

Runonce.exe /AlternateShellStartup

<b>Use case:</b>	Persistence, bypassing defensive counter measures
<b>Privileges required:</b>	Administrator
<b>Operating systems:</b>	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1218