.. /Runexehelper.exe

Execute

Launcher process

Paths:
c:\windows\system32\runexehelper.exe

Resources:
- https://twitter.com/0gtweet/status/1206692239839289344

Acknowledgements:
- Grzegorz Tworek (@0gtweet)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/197615345b927682ab7ad7fa3c5f5bb2ed911eed/rules/windows/process_creation/proc_creation_win_lolbin_runexehelper.yml
- IOC: c:\windows\system32\runexehelper.exe is run
- IOC: Existence of runexewithargs_output.txt file

Execute

Launches the specified exe. Prerequisites: (1) diagtrack_action_output environment variable must be set to an existing, writable folder; (2) runexewithargs_output.txt file cannot exist in the folder indicated by the variable.

```
runexehelper.exe c:\windows\system32\calc.exe
```

Use case:	Executes arbitrary code
Privileges required:	User
Operating systems:	Windows 10, Windows 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022
ATT&CK® technique:	T1218