.. /OfflineScannerShell.exe

Execute (DLL)

Windows Defender Offline Shell

Paths:
C:\Program Files\Windows Defender\Offline\OfflineScannerShell.exe

Acknowledgements:
- Elliot Killick (@elliotkillick)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/bea6f18d350d9c9fdc067f93dde0e9b11cc22dc2/rules/windows/process_creation/proc_creation_win_lolbas_offlinescannershell.yml
- IOC: OfflineScannerShell.exe should not be run on a normal workstation

Execute

Execute mpclient.dll library in the current working directory

```
OfflineScannerShell
```

Use case:	Can be used to evade defensive countermeasures or to hide as a persistence mechanism
Privileges required:	Administrator
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1218
Tags:	Execute: DLL