.. /DefaultPack.EXE

Execute

This binary can be downloaded along side multiple software downloads on the microsoft website. It gets downloaded when the user forgets to uncheck the option to set Bing as the default search provider.

Paths:
C:\Program Files (x86)\Microsoft\DefaultPack\DefaultPack.exe

Resources:
- https://twitter.com/checkymander/status/1311509470275604480.

Acknowledgements:
- checkymander (@checkymander)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_lolbin_defaultpack.yml
- IOC: DefaultPack.EXE spawned an unknown process

Execute

Use DefaultPack.EXE to execute arbitrary binaries, with added argument support.

```
DefaultPack.EXE /C:"process.exe args"
```

Use case:	Can be used to execute stagers, binaries, and other malicious commands.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1218