.. /winget.exe

Execute Download

Windows Package Manager tool

Paths:
C:\Users\user\AppData\Local\Microsoft\WindowsApps\winget.exe

Resources:

- https://saulpanders.github.io/2022/01/02/New-Year-New-LOLBAS.html
- https://docs.microsoft.com/en-us/windows/package-manager/winget/#production-recommended

Acknowledgements:

- Paul (@saulpanders)
- Konrad 'unrooted' Klawikowski

Detections:

- IOC: winget.exe spawned with local manifest file
- IOC: Sysmon Event ID 1 - Process Creation
- Analysis: https://saulpanders.github.io/2022/01/02/New-Year-New-LOLBAS.html
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_winget_local_install_via_manifest.yml

Execute

Downloads a file from the web address specified in manifest.yml and executes it on the system. Local manifest setting must be enabled in winget for it to work: `winget settings --enable LocalManifestFiles`

```
winget.exe install --manifest manifest.yml
```

Use case:	Download and execute an arbitrary file from the internet
Privileges required:	Local Administrator - required to enable local manifest setting
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1105

Download

Download and install any software from the Microsoft Store using its name or Store ID, even if the Microsoft Store App itself is blocked on the machine. For example, use "Sysinternals Suite" or `9p7knl5rwt25` for obtaining ProcDump, PsExec via the Sysinternals Suite. Note: a Microsoft account is required for this.

```
winget.exe install --accept-package-agreements -s msstore [name or ID]
```

Use case:	Download and install software from Microsoft Store, even if Microsoft Store App is blocked
Privileges required:	User
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1105