.. /OneDriveStandaloneUpdater.exe

☆ Star 7,060

Download

OneDrive Standalone Updater

Paths:
C:\Users\<username>\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe

Resources:
- https://github.com/LOLBAS-Project/LOLBAS/pull/153

Acknowledgements:
- Elliot Killick (@elliotkillick)

Detections:
- IOC: HKCU\Software\Microsoft\OneDrive\UpdateOfficeConfig\UpdateRingSettingURLFromOC being set to a suspicious non-Microsoft controlled URL
- IOC: Reports of downloading from suspicious URLs in %localappdata%\OneDrive\setup\logs\StandaloneUpdate_*.log files
- Sigma: registry_set_lolbin_onedrivestandaloneupdater.yml

Download

Download a file from the web address specified in HKCU\Software\Microsoft\OneDrive\UpdateOfficeConfig\UpdateRingSettingURLFromOC. ODSUUpdateXMLUrlFromOC and UpdateXMLUrlFromOC must be equal to non-empty string values in that same registry key. UpdateOfficeConfigTimestamp is a UNIX epoch time which must be set to a large QWORD such as 99999999999 (in decimal) to indicate the URL cache is good. The downloaded file will be in %localappdata%\OneDrive\StandaloneUpdater\PreSignInSettingsConfig.json

```
OneDriveStandaloneUpdater
```

Use case:	Download a file from the Internet without executing any anomalous executables with suspicious arguments
Privileges required:	User
Operating systems:	Windows 10
ATT&CK® technique:	T1105: Ingress Tool Transfer