.. /cmdl32.exe

Download

Microsoft Connection Manager Auto-Download

Paths:
C:\Windows\System32\cmdl32.exe
C:\Windows\SysWOW64\cmdl32.exe

Resources:
- https://github.com/LOLBAS-Project/LOLBAS/pull/151
- https://twitter.com/ElliotKillick/status/1455897435063074824
- https://elliotonsecurity.com/living-off-the-land-reverse-engineering-methodology-plus-tips-and-tricks-cmdl32-case-study/

Acknowledgements:
- Elliot Killick (@elliotkillick)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_cmdl32.yml
- IOC: Reports of downloading from suspicious URLs in %TMP%\config.log
- IOC: Useragent Microsoft(R) Connection Manager Vpn File Update

Download

Download a file from the web address specified in the configuration file. The downloaded file will be in %TMP% under the name VPNXXXX.tmp where "X" denotes a random number or letter.

```
cmdl32 /vpn /lan %cd%\config
```

Use case: Download file from Internet
Privileges required: User
Operating systems: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1105