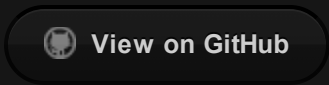


./ persistence-info.github.io



Code Signing DLL

Location:

```
>> HKLM\SOFTWARE\Microsoft\Cryptography\Providers
>> HKLM\SOFTWARE\Microsoft\Cryptography\OID
```

Classification:

Criteria	Value
Permissions	Admin
Security context	User
Persistence type	Registry
Code type	DLL
Launch type	User initiated ¹
Impact	Non-destructive
OS version	All OS versions
Dependencies	OS only
Toolset	Scriptable

Description:

Hijack attacks [...] permit persistent code execution in the context of any application that performs code signing or signature validation. By implementing a SIP or trust provider, code execution is possible.

References:

```
>> https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf
>> Open-source implementation
```

Credits:

[Matt Graeber](#)

See also:

Remarks:

1. All cases of signature verification, including UAC prompts and displaying file properties. [↵](#)