./ persistence-info.github.io

View on GitHub

AMSI Providers

Location:

>> `HKLM\SOFTWARE\Microsoft\AMSI\Providers`
>> `HKLM\SOFTWARE\Classes\CLSID`

Classification:

Criteria	Value
Permissions	Admin
Security context	User; System
Persistence type	Registry
Code type	DLL[1]
Launch type	Automatic
Impact	Non-destructive
OS Version	All OS versions
Dependencies	OS only
Toolset	Scriptable

Description:

> AMSI is designed in particular to combat “fileless malware”. Application types that can optimally leverage AMSI technology include script engines, applications that need memory buffers to be scanned before using them, and applications that process files that can contain non-PE executable code (such as Microsoft Word and Excel macros, or PDF documents).
>
> As a creator of antimalware products, you can choose to author and register your own in-process COM server (a DLL) to function as an AMSI provider.

References:

>> https://docs.microsoft.com/en-us/windows/win32/amsi/dev-audience
>> https://twitter.com/0gtweet/status/1452680501249069062
>> Sample open source DLL

Credits:

See also:

Remarks:

1. COM ↩