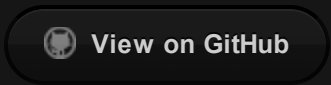


./ persistence-info.github.io



LSA Extension

Location:

HKLM\SYSTEM\CurrentControlSet\Control\LsaExtensionConfig\LsaSrv

Classification:

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

Description:

The REG_MULTI_SZ value named Extensions contains filenames of DLLs being automatically loaded by lsass.exe. Each DLL has its InitializeLsaExtension() method called after loading.

References:

https://twitter.com/0gtweet/status/1476286368385019906

Credits:

0gtweet

See also:

Remarks:

- TrustedInstaller required ↩