


←

Post



eral4m

@eral4m

...

#lolbin / #lolbas for file copy:

colorcpl.exe c:\windows\system32\calc.exe

Copies file to c:\windows\system32\spool\drivers\color\calc.exe

Can evasively move files out of commonly abused staging areas via a process not normally monitored.

Det logic below

C:\Windows\system32\cmd.exe

C:\>colorcpl c:\windows\system32\calc.exe

C:\>

Managecolor

areViewApp Tools

This PC > Local Disk (C:) > Windows > System32 > spool > drivers > color

Name	Date modified	Type	Size
AdobeRGB2003.icc	20/08/2021 13:32	ICC Profile	282
calc.exe	07/12/2019 09:09	Application	27
D50.camp	07/12/2019 09:08	WCS Viewing Con...	2
D65.camp	07/12/2019 09:08	WCS Viewing Con...	2
Graphics.gmmp	07/12/2019 09:08	WCS Gamut Map...	1
MediaSim.gmmp	07/12/2019 09:08	WCS Gamut Map...	1
New Bitmap Image.bmp	20/08/2021 10:50	BMP File	0
Photo.gmmp	07/12/2019 09:08	WCS Gamut Map...	1
Proofing.gmmp	07/12/2019 09:08	WCS Gamut Map...	1
RSWOP.icm	07/12/2019 09:08	ICC Profile	213
sRGB Color Space Profile.icm	07/12/2019 09:08	ICC Profile	4
wscRGB.cdmp	07/12/2019 09:08	WCS Device Profile	17
wsRGB.cdmp	07/12/2019 09:08	WCS Device Profile	2

10:17 AM · Jan 10, 2022

1

Repost

3

Likes

1

Bookmark

💬

↺↻


❤️


🔖1

↑

New to X?

Sign up now to get your own personalized timeline!

 Sign up with Google

 Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.

↺ Retry

[Terms of Service](#)

[Privacy Policy](#)

[Cookie Policy](#)

[Accessibility](#)

[Ads info](#)

[More ...](#)

© 2024 X Corp.

Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.

For more details, see our Privacy Policy: <https://x.com/en/privacy>

×

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies