




Settings



Post



Nasreddine Bencherchali  @nas\_bench



Another fun fact about adplus is that you can use it via a config file by using the "-c" flag to execute commands or dump memory (Just replace notepad with lsass in this example) [#lolbin](#) [#lolbas](#)

adplus.exe -c [ConfigFile]

The media could not be played.

Reload



Nasreddine Bencherchali  @nas\_bench · Jun 9, 2022

We know from LOLBAS that adplus can be used to dump lsass (lolbas-project.github.io/lolbas/OtherMS...). But you can also use it to run arbitrary commands and binaries with the "-sc" flag. [#lolbin](#) [#lolbas](#)

adplus.exe -crash -o [OutputDir] -sc [Command]

The media could not be played.

Reload

5:13 PM · Jun 9, 2022

7 Reposts 1 Quote 15 Likes 3 Bookmarks



3



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