



Settings



Post



Samir
@SBousseaden



this is a very cool approach to dump procmem, expect to see it enrolled (if not already) into upcoming attacks, same artifacts (ProcAcess)+ cmdline contains "minidump" for ProcessCreation:

[modexp.wordpress.com/2019/08/30/min...](https://modexp.wordpress.com/2019/08/30/minidump/)



2:41 PM · Aug 30, 2019

45 Reposts 1 Quote 95 Likes 13 Bookmarks



13



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