

X

Settings

← Post

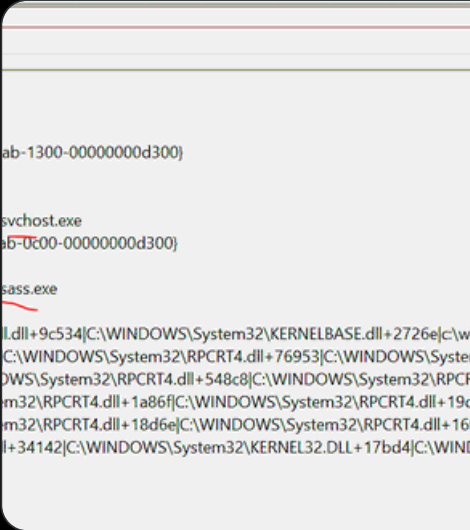


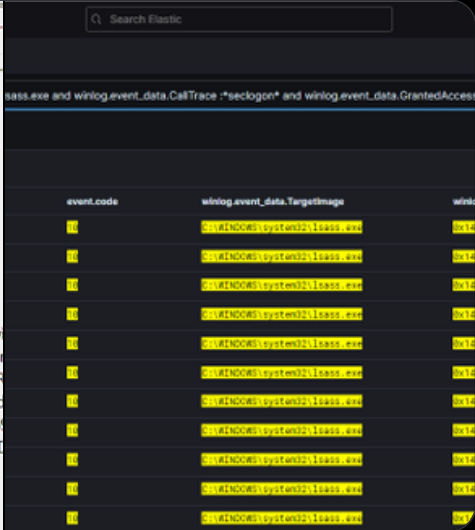
Samir
@SBousseaden


...


Sysmon 10 with CallTrace contains seclogon (abused svc via fake client pid) + GAccess eq 14C0 & target is lsass is high likely an indicator of lsass handle obtention using malseclogon:

PROCESS_CREATE_PROCESS
PROCESS_DUP_HANDLE
PROCESS_QUERY_INFORMATION







Antonio Cocomazzi  @splinter_code · Jun 28, 2022

My blog series "The hidden side of Seclogon" continues with part 3: Racing for LSASS dumps 🔥

Enjoy the read :D

...

[Show more](#)

1:04 AM · Jun 29, 2022

35 Reposts 92 Likes 18 Bookmarks









 18



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