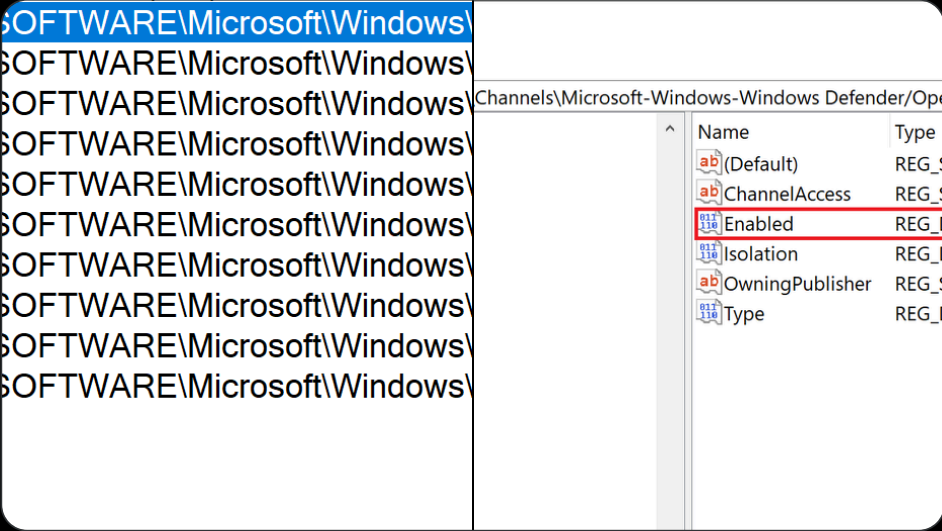✕

Settings

⚙ Settings

← Post

Arda Büyükkaya ✓
@WhichbufferArda

Lockbit Black 3.0 can yeet the Windows Defender and Event logs of it. Look at the Enabled key, it's set to 0 by Ransomware at the start.
@vxunderground @malwrhunterteam

SOFTWARE\Microsoft\Windows\
SOFTWARE\Microsoft\Windows\
SOFTWARE\Microsoft\Windows\   Channels\Microsoft-Windows-Windows Defender/Ope
SOFTWARE\Microsoft\Windows\
SOFTWARE\Microsoft\Windows\   Name   Type
SOFTWARE\Microsoft\Windows\   ab (Default)   REG_S
SOFTWARE\Microsoft\Windows\   ab ChannelAccess   REG_S
SOFTWARE\Microsoft\Windows\   Enabled   REG_D
SOFTWARE\Microsoft\Windows\   Isolation   REG_D
SOFTWARE\Microsoft\Windows\   ab OwningPublisher   REG_S
                                    Type   REG_D

12:12 PM · Jul 4, 2022

97 Reposts   **7** Quotes   **296** Likes   **56** Bookmarks

💬   🔁   ♡   🔖 56   ⬆

New to X?

Sign up now to get your own personalized timeline!

🔵 Sign up with Google

 Sign up with Apple

Create account

Something went wrong. Try reloading.

↻ Retry

Don't miss what's happening
People on X are the first to know.

Log in   Sign up

Welcome to x.com!   ✕

Did someone say … cookies?

Accept all cookies

Refuse non-essential cookies