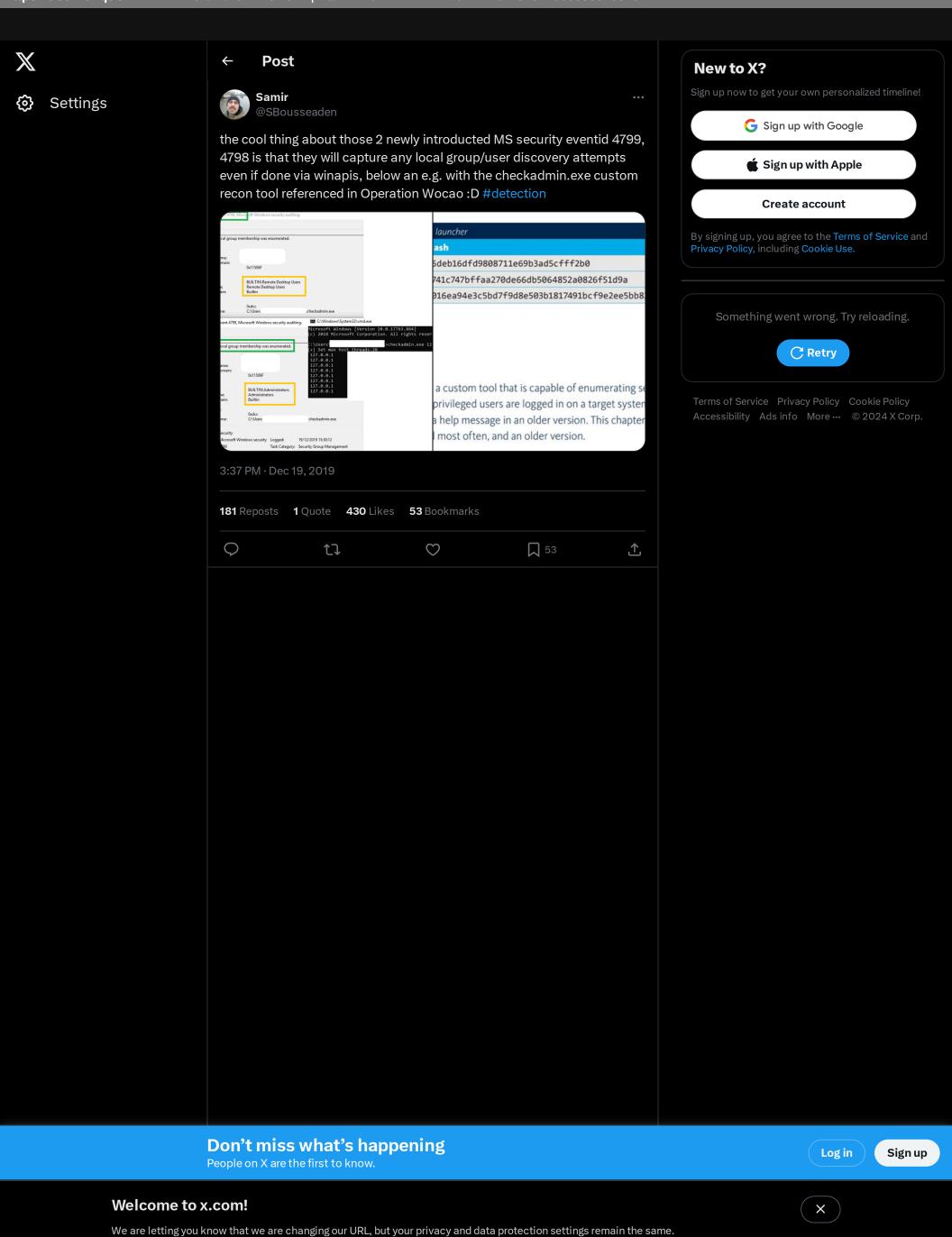
Samir on X: "the cool thing about those 2 newly introducted MS security eventid 4799, 4798 is that they will capture any local group/user discovery attempts even if done via winapis, below an e.g. with the checkadmin.exe custom recon tool referenced in Operation Wocao :D #detection https://t.co/E0vq8GkW7I" / X - 02/11/2024 18:10 https://x.com/SBousseaden/status/1207671369963646976



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.

For more details, see our Privacy Policy: https://x.com/en/privacy

Accept all cookies

Refuse non-essential cookies