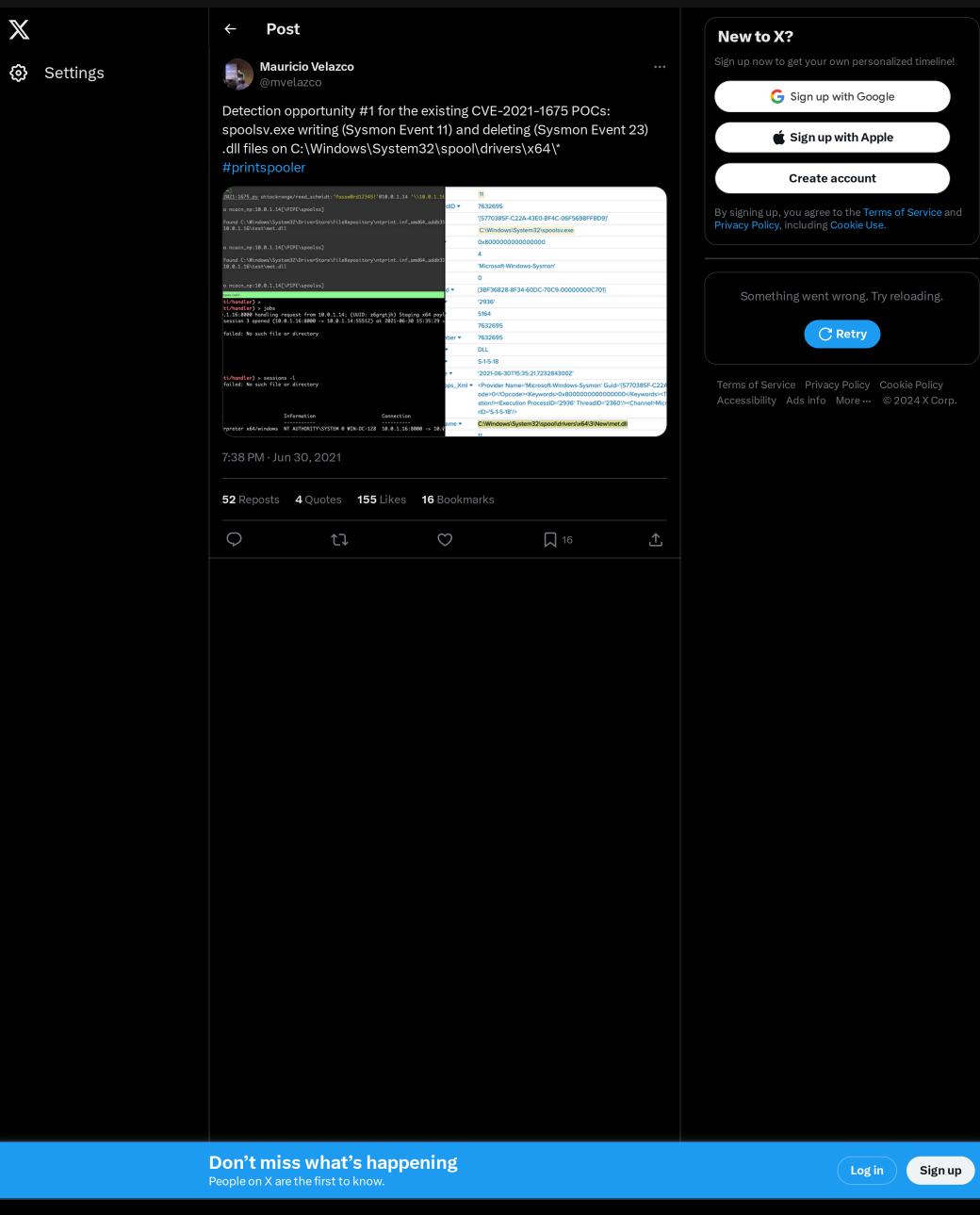X

⚙ Settings

← Post

Mauricio Velazco
@mvelazco

Detection opportunity #1 for the existing CVE-2021-1675 POCs: spoolsv.exe writing (Sysmon Event 11) and deleting (Sysmon Event 23) .dll files on C:\Windows\System32\spool\drivers\x64*
#printspooler

7:38 PM · Jun 30, 2021

52 Reposts   4 Quotes   155 Likes   16 Bookmarks

💬   🔁   ♡   🔖 16   ⬆