



Settings



Post

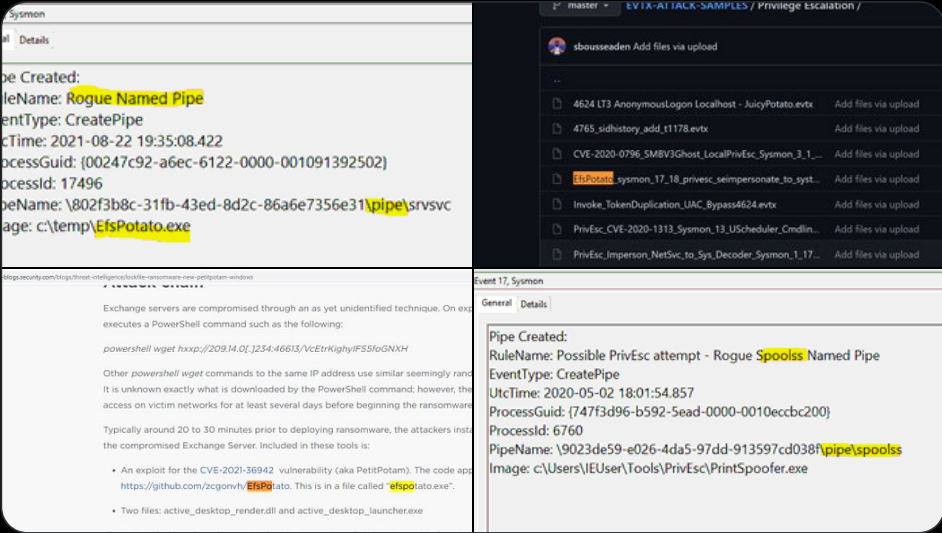


Samir
@SBousseaden



added main detection artifact for EfsPotato (privesc via Selmpersonate to System with rogue named pipe) (same trick used for fake Spoolss privesc) - for #sysmon users add this to your config (Pipe Events)

<PipeName condition="contains" name="Rogue Named Pipe">\pipe\
</PipeName>



9:45 PM · Aug 22, 2021

19 Reposts 66 Likes 13 Bookmarks



13



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