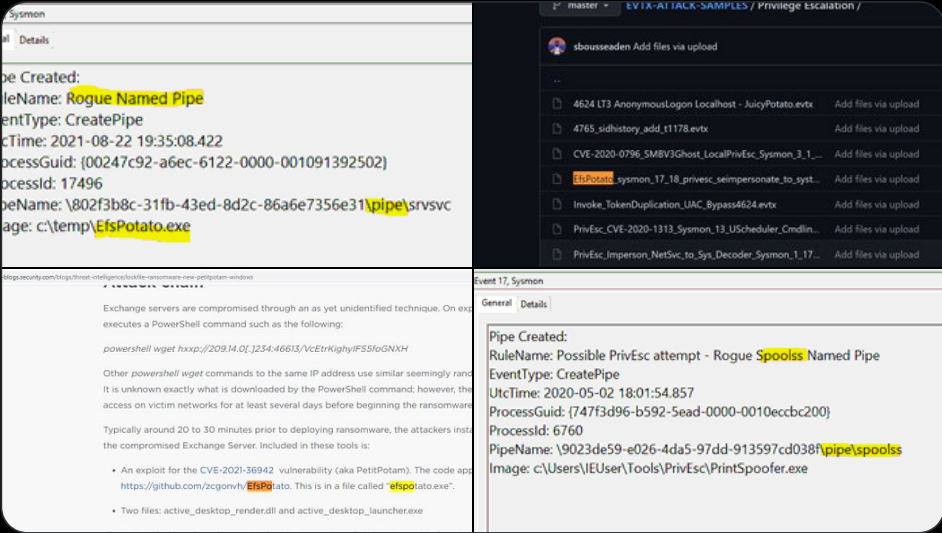X

Settings

Post

Samir
@SBousseaden

added main detection artifact for EfsPotato (privesc via SeImpersonate 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

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!
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