Suricata - Bug #5160

smb: Misguiding keyword smb.named_pipe

02/24/2022 12:34 PM - Eloy Pérez

Status: New
Priority: Normal
Assignee: OISF Dev
Category: TBD
Target version: TBD
Affected Versions: TBD
Effort: TBD

Description

The "smb.named_pipe" this keyword is used to match shares in the tree_connect request that contains named pipes (such as the IPC$).

I think here we are not using the proper terminology because IPC$ is not a named pipe, **IPC$ is a pipe share, the share used to access named pipes.** The named pipes themselves are those "special files" under IPC$ used to connect with an specific service in the target machine, like "samr", "lsarpc", etc.

Therefore I think the name of the keyword is misleading and something like "smb.pipe_share" would be more accurate.