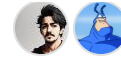


also see a `SrcProcParentName` for parent?



 **nasbench** self-assigned this on Dec 2, 2022

 **nasbench** added the **Author Input Required** label on Dec 2, 2022



s7ryph commented on Dec 5, 2022

Author



Apologize, I see how the naming convention is confusing. In the example `SrcProcName` = Parent and `TgtProcName` = Image as they would appear in a Windows log. In this situation the `SrcProcName` would be launching the `TgtProcName` process and passing the command. `SrcProcParentName` would be the Grandparent.

And yes I am referring to [Mavinject Inject DLL Into Running Process](#) and the SentinelOne is also T1055 Process Injection, I should have specified.





nasbench commented on Dec 5, 2022

Member



Thanks for the clarification. Will add some filters to the rule in a bit.

 **nasbench** removed the **Author Input Required** label on Dec 5, 2022

 **nasbench** added a commit to nasbench/sigma that referenced this issue on Dec 6, 2022

 fix: fix issue [SigmaHQ#3742](#)

3bcce88



nasbench mentioned this issue on Dec 6, 2022

feat: new rules and fixes #3759

Merged



frack113 closed this as completed in [#3759](#) on Dec 6, 2022

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.