





Sign in


 SigmaHQ / **sigma**


Public


 Notifications


 Fork 2.2k


 Star 8.3k


 Code


 Issues 11


 Pull requests 35

 Discussions

 Actions

 Wiki

 Security




Exemption on proc_creation_win_creation_mavinject_process_injection.yml #3742

New issue

 Closed

 s7ryph opened this issue on Nov 30, 2022 · 3 comments · Fixed by [#3759](#)



s7ryph commented on Nov 30, 2022

...


mavinject process should be excluded from devices running App-V as it is normal behavior. From [LOLBAS Project](#)

IOC: mavinject.exe should not run unless APP-v is in use on the workstation

The logic can also be found in the rule on [SentinelOne](#)

Recommend adding ParentImage Not EndsWith '/AppVClient.exe' to the rule to reduce potential false positives.

Assignees

 nasbench

Labels

None yet

Projects


None yet

Milestone


No milestone

Development

Successfully merging a pull request may close this issue.

 feat: new rules and fixes
nasbench/sigma

2 participants



nasbench commented on Dec 2, 2022

Member

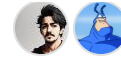
...

Hi,

Thanks for opening the issue. Can you please confirm that you're referring to this rule [Mavinject Inject DLL Into Running Process](#)

Also, in the SentinelOne link you mentioned what's the `SrcProcName` referring to? I don't think it's the parent, since I

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.