


Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing


Q


Sign in


Sign up

SigmaHQ / sigma


Public

Sponsor

Notifications

Fork

2.2k

Star

8.3k


<> CodeIssues 11Pull requests 33DiscussionsActionsWikiSecurityInsights

Cobalt Strike Default Pipes #253

New issue

✓ Closed

mschilt opened this issue on Feb 21, 2019 · 2 comments




mschilt commented on Feb 21, 2019 • edited ▾

...

Addition to sysmon_mal_namedpipes.yml:

CS default named pipes:
msagent_#number used by SMB Beacon's peer-to-peer communication.
status_#number used by SMB Beacon's named pipe stager


Ref:
<https://blog.cobaltstrike.com/2019/02/19/cobalt-strike-team-server-population-study/>
<https://www.cobaltstrike.com/help-malleable-c2>



Neo23x0 commented on Feb 21, 2019

Collaborator ...


I'll add the `msagent_` named pipe, but I am unsure about the `status_` named pipe. My guess is that it would cause many false positives if it gets implemented as `status_*`.



Neo23x0 pushed a commit that referenced this issue on Feb 21, 2019

Rule: suspicious pipes extended ...


d3b623e




mschilt commented on Feb 25, 2019

Author ...

Don't think there will be a lot of FPs as long as its not `*status_*`.



thomaspatzke closed this as completed on Apr 1, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet




Milestone

No milestone

Development

No branches or pull requests

3 participants



Sign up for free

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