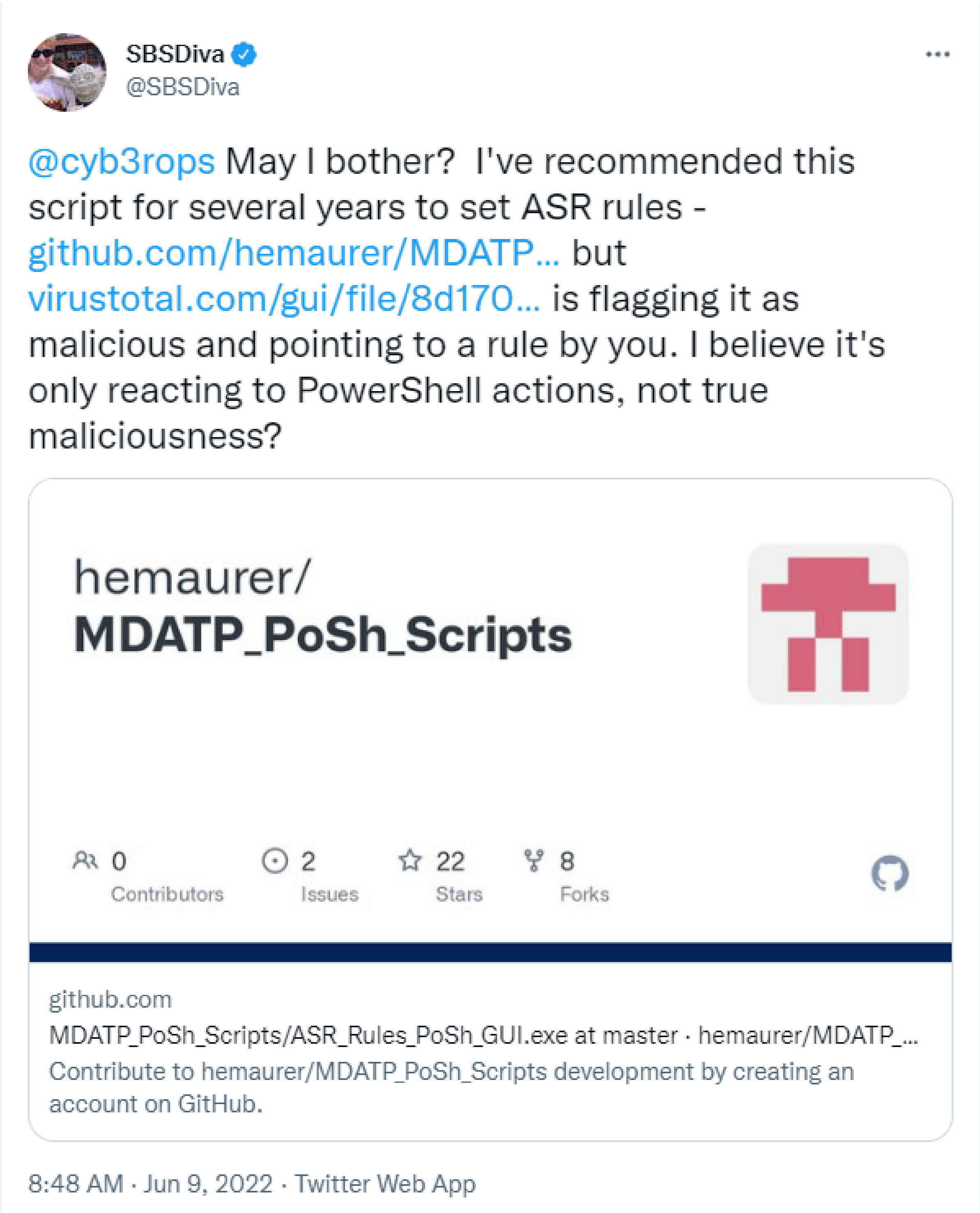


SBSDiva
@SBSDiva

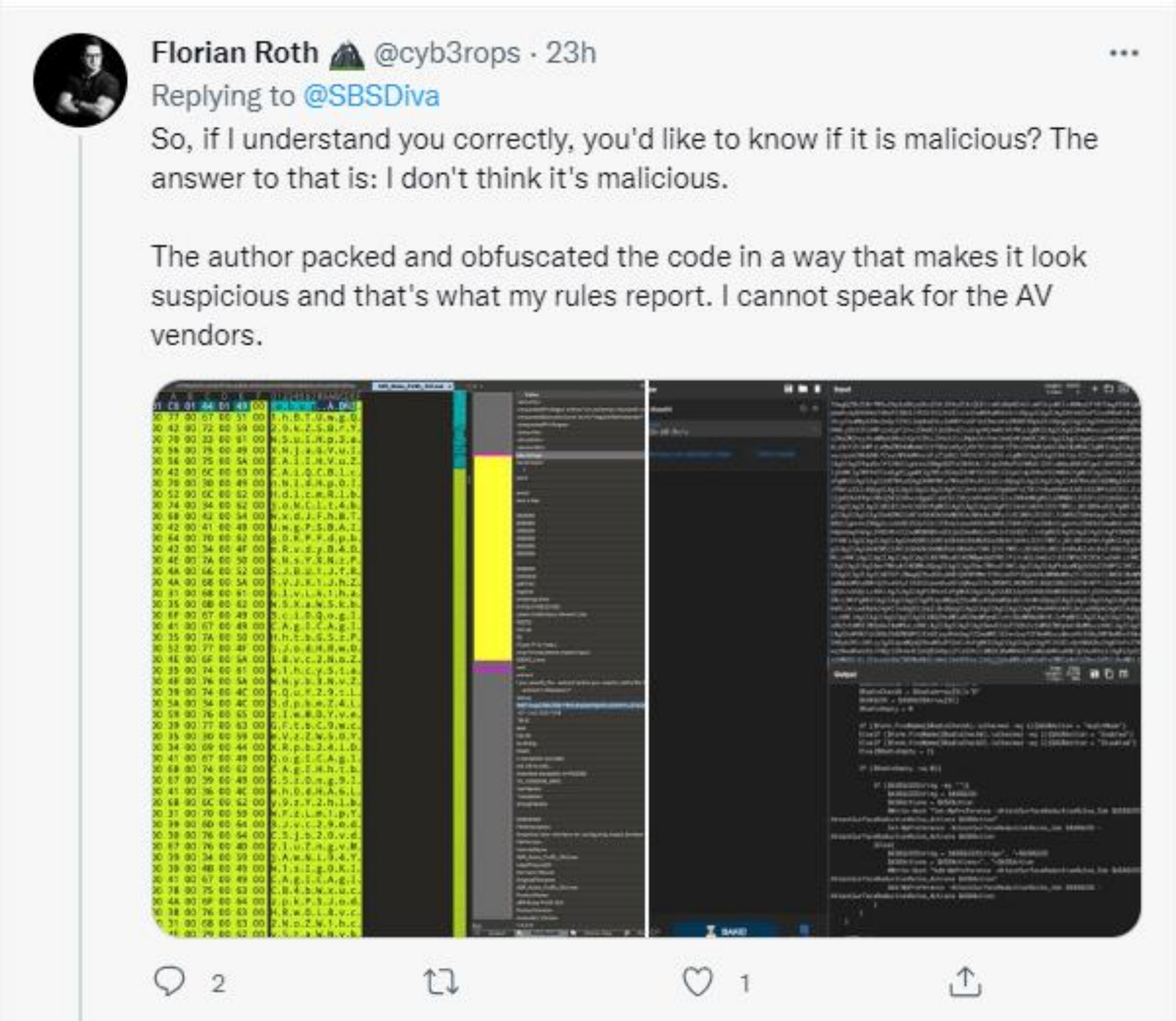
@cyb3rops May I bother? I've recommended this script for several years to set ASR rules - github.com/hemaurer/MDATP… but virustotal.com/gui/file/8d170… is flagging it as malicious and pointing to a rule by you. I believe it's only reacting to PowerShell actions, not true maliciousness?

hemaurer/
MDATP_PoSh_Scripts

0 Contributors · 2 Issues · 22 Stars · 8 Forks

github.com
MDATP_PoSh_Scripts/ASR_Rules_PoSh_GUI.exe at master · hemaurer/MDATP_...
Contribute to hemaurer/MDATP_PoSh_Scripts development by creating an account on GitHub.

8:48 AM · Jun 9, 2022 · Twitter Web App

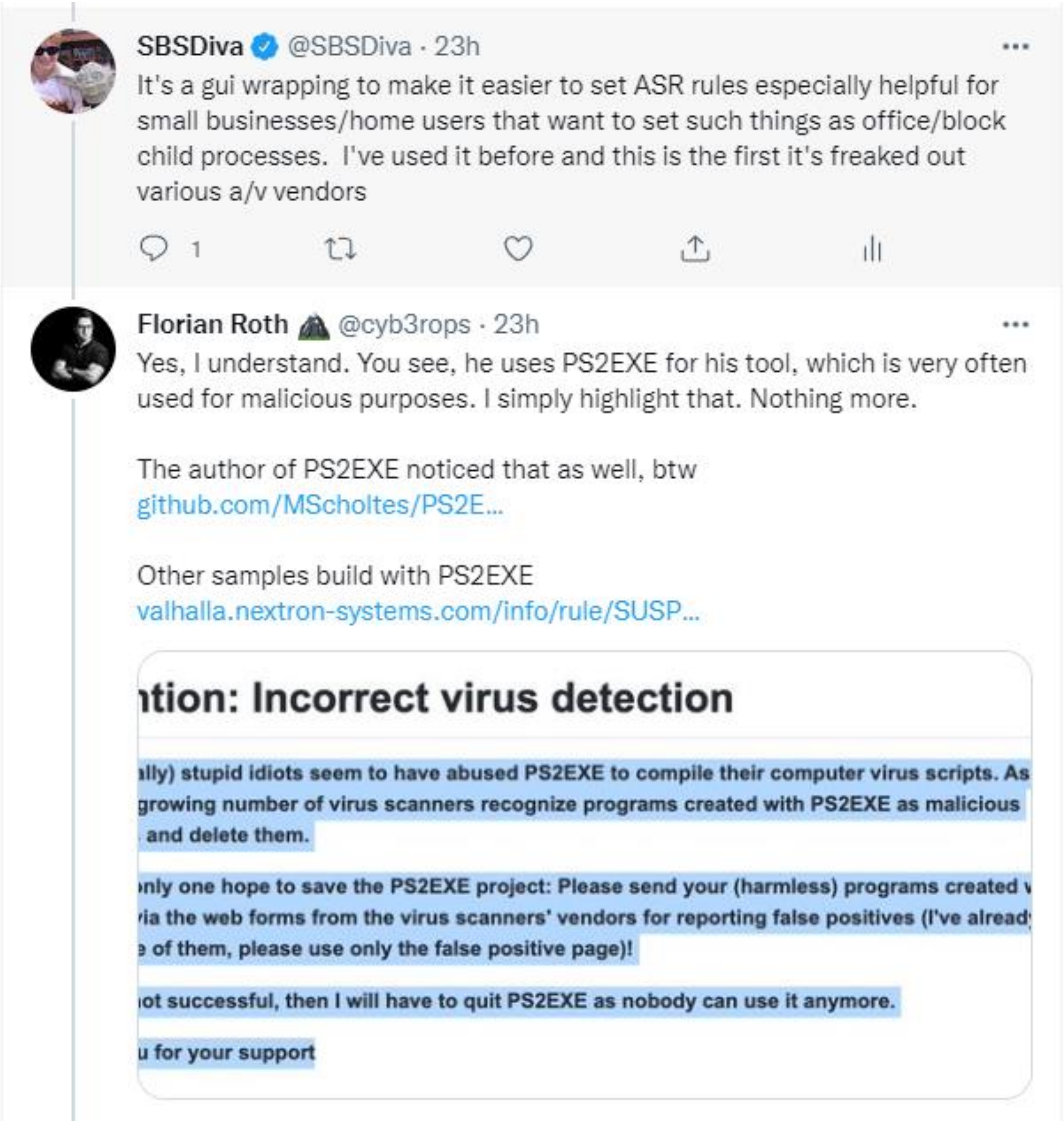


Florian Roth @cyb3rops · 23h

Replying to @SBSDiva

So, if I understand you correctly, you'd like to know if it is malicious? The answer to that is: I don't think it's malicious.

The author packed and obfuscated the code in a way that makes it look suspicious and that's what my rules report. I cannot speak for the AV vendors.



SBSDiva @SBSDiva · 23h

It's a gui wrapping to make it easier to set ASR rules especially helpful for small businesses/home users that want to set such things as office/block child processes. I've used it before and this is the first it's freaked out various a/v vendors

Florian Roth @cyb3rops · 23h

Yes, I understand. You see, he uses PS2EXE for his tool, which is very often used for malicious purposes. I simply highlight that. Nothing more.

The author of PS2EXE noticed that as well, btw
github.com/MScholtes/PS2E...

Other samples build with PS2EXE
valhalla.nextron-systems.com/info/rule/SUSP...

ıtion: Incorrect virus detection

ılly) stupid idiots seem to have abused PS2EXE to compile their computer virus scripts. As growing number of virus scanners recognize programs created with PS2EXE as malicious and delete them.

ınly one hope to save the PS2EXE project: Please send your (harmless) programs created v ɪia the web forms from the virus scanners' vendors for reporting false positives (I've alread e of them, please use only the false positive page)!

ıot successful, then I will have to quit PS2EXE as nobody can use it anymore.

u for your support