Post

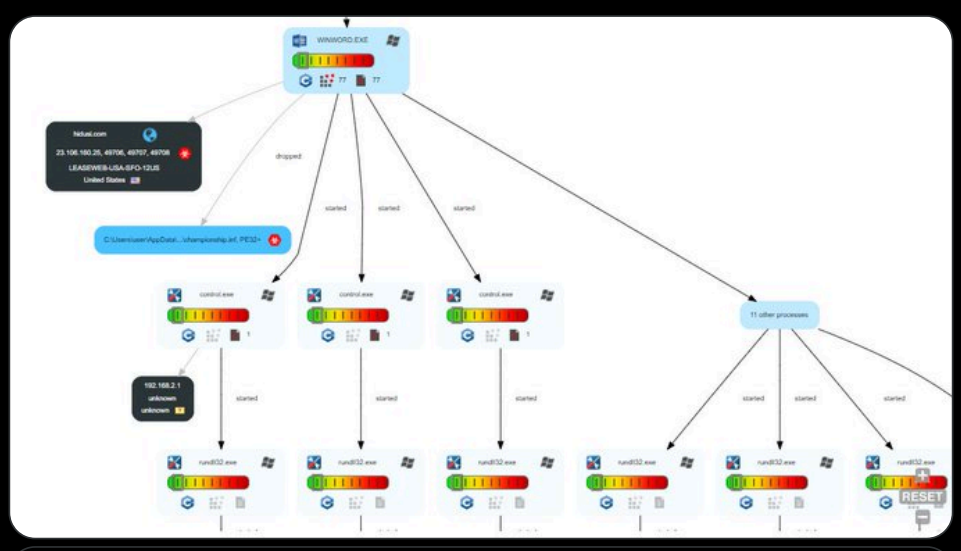
neonprimetime
@neonprimetime

sample mentioned in sigma rule from @JAMESWT_MHT

bazaar.abuse.ch/sample/938545f...

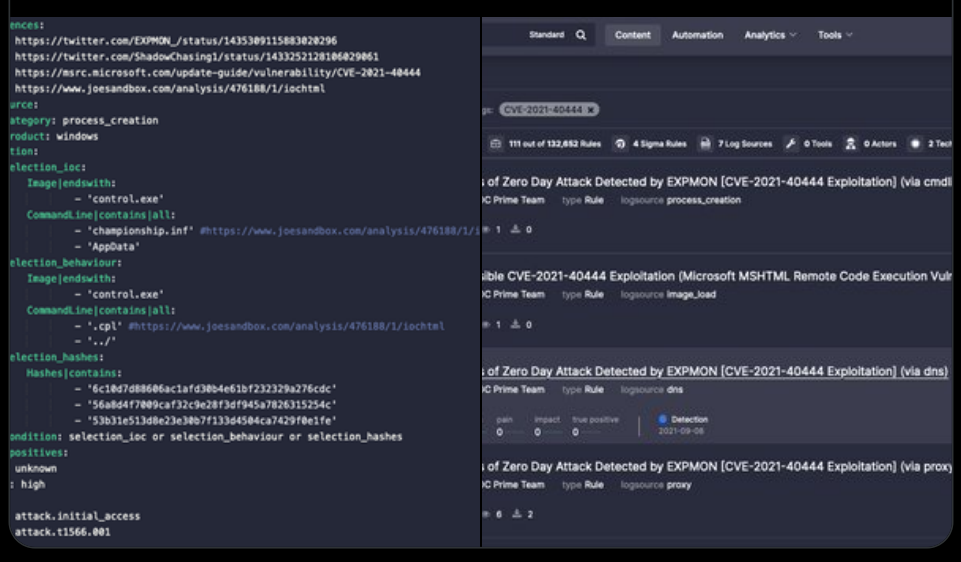
app.any.run/tasks/36c14029...

md5 1d2094ce85d66878ee079185e2761beb



Ring3API @ntlmrelay · Sep 8, 2021

Another #IOC-Based free #Sigma which included this behavior. @RedDrip7 nice find! this also tracked by @joe4security sandbox.
➡️tdm.socprime.com/tdm/info/vzmHh...
+ one more #ThreatHunting rule available by tag: ➡️tdm.socprime.com/?tagsCustom=CV.....
Show more



2:41 PM · Sep 8, 2021

8 Reposts 1 Quote 15 Likes 1 Bookmark

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Something went wrong. Try reloading.

Retry