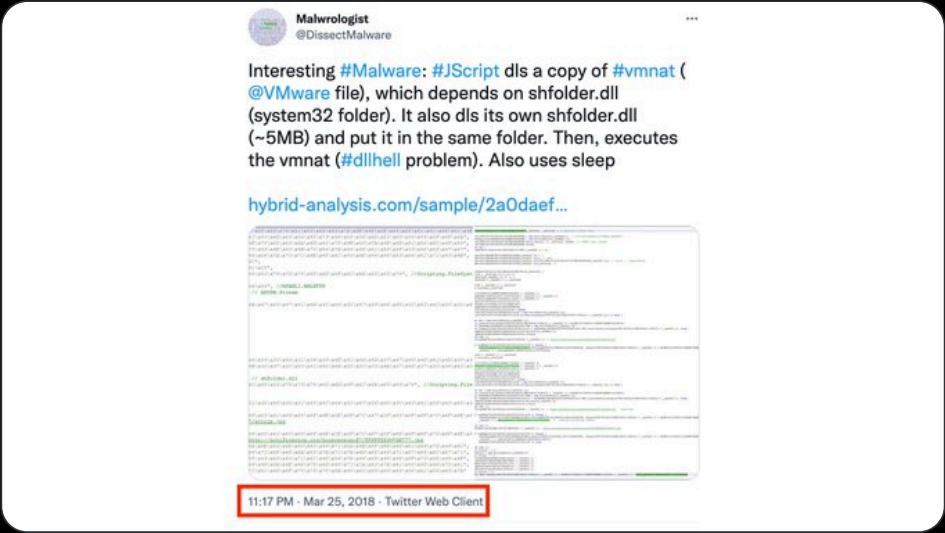Stephan Berger on X: "1/ #ThreatHunting: TA's has used the legitimate VMWare binary vmnat.exe for side-loading malicious DLLs for years (2018?). The #Mekotio Banker also uses this technique to load malicious code to fool security products. Following some background & hunting tips. 💡 📝 #dfir https://t.co/MKWL4qbfEz" / X - 02/11/2024 16:35 https://x.com/malmoeb/status/1525901219247845376

X

Settings

← Post

Stephan Berger ✔
@malmoeb

1/ #ThreatHunting: TA's has used the legitimate VMWare binary vmnat.exe for side-loading malicious DLLs for years (2018?).

The #Mekotio Banker also uses this technique to load malicious code to fool security products.

Following some background & hunting tips. 💡🧵

#dfir

Malwrologist
@DissectMalware

Interesting #Malware: #JScript dls a copy of #vmnat (@VMware file), which depends on shfolder.dll (system32 folder). It also dls its own shfolder.dll (~5MB) and put it in the same folder. Then, executes the vmnat (#dllhell problem). Also uses sleep

hybrid-analysis.com/sample/2a0daef...

11:17 PM · Mar 25, 2018 · Twitter Web Client

8:09 PM · May 15, 2022

41 Reposts **113** Likes **37** Bookmarks

💬 🔁 ♡ 🔖 37 ⬆

New to X?

Sign up now to get your own personalized timeline!

G 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

Don't miss what's happening
People on X are the first to know.

Log in Sign up