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 & amp; hunting tips. 💡 **#dfir https://t.co/MKWL4qbfEz" / X** - 02/11/2024 16:35 https://x.com/malmoeb/status/1525901219247845376 **Post** New to X? Sign up now to get your own personalized timeline! Stephan Berger 🕏 Settings G Sign up with Google 1/ #ThreatHunting: TA's has used the legitimate VMWare binary vmnat.exe for side-loading malicious DLLs for years (2018?). Sign up with Apple The #Mekotio Banker also uses this technique to load malicious code to **Create account** fool security products. Following some background & hunting tips. 💡 📃 Privacy Policy, including Cookie Use. #dfir Something went wrong. Try reloading. Interesting #Malware: #JScript dls a copy of #vmnat ( @VMware file), which depends on shfolder.dll **C** Retry (system32 folder). It also dls its own shfolder.dll (~5MB) and put it in the same folder. Then, executes the vmnat (#dlihell problem). Also uses sleep hybrid-analysis.com/sample/2a0daef... Terms of Service Privacy Policy Cookie Policy Accessibility Ads info More ... © 2024 X Corp. 8:09 PM · May 15, 2022 41 Reposts 113 Likes 37 Bookmarks Q **€**Ţ  $\bigcirc$  $\square$  37 土

## Don't miss what's happening

People on X are the first to know.

Log in

Sign up

## Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same. For more details, see our Privacy Policy: <a href="https://x.com/en/privacy">https://x.com/en/privacy</a>

## Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. Show more about your choices.

Accept all cookies

Refuse non-essential cookies