Settings

← Post

Wietze
@Wietze

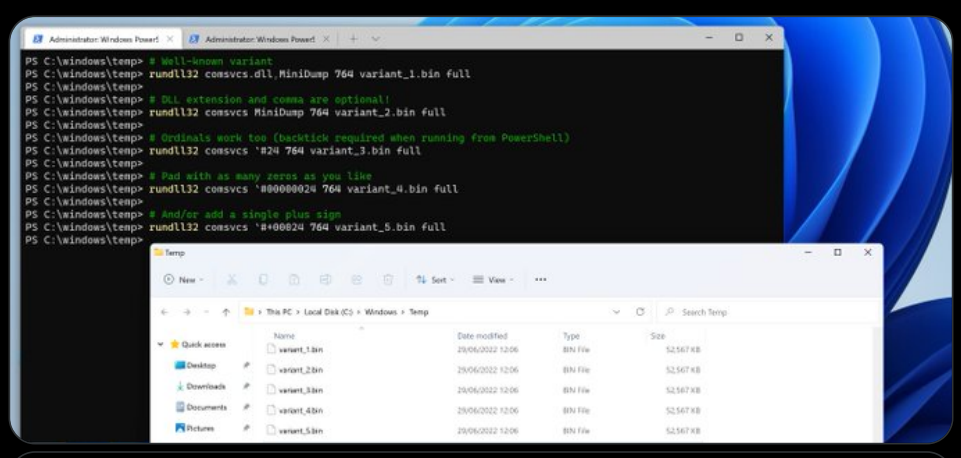
#HuntingTipOfTheDay

⚔️ Attackers love comsvcs to dump LSASS. Ensure your hunts/detections are resilient.

Did you know about (padded) ordinals, missing extensions/commas?

⚠️ Variant 4 is not blocked by Defender!

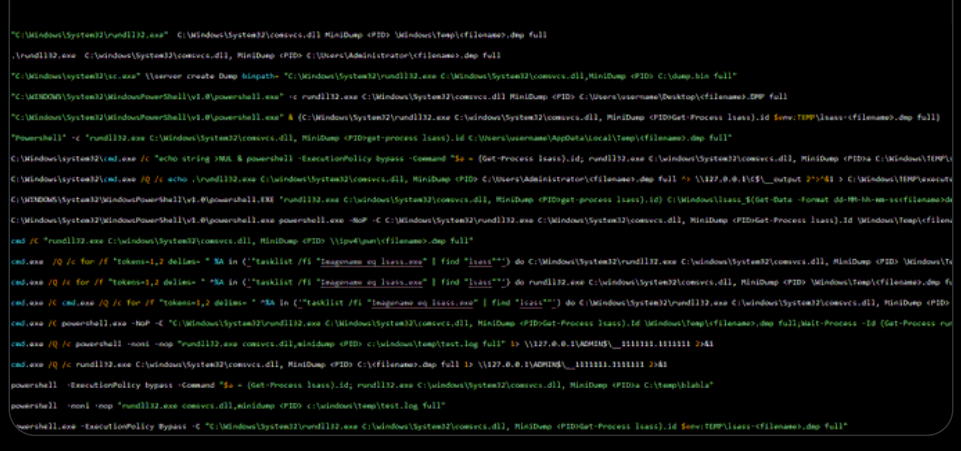
Related 🐦: x.com/cyb3rops/statu...



John Lambert @JohnLaTwC · Jun 23, 2021

#HuntingTipOfTheDay
Search for command lines 🔎with 'comsvcs.dll' and 'MiniDump' to find credential dumping. 👀

✏️Test your detections: gist.github.com/JohnLaTwC/3e7d.....
Show more



1:27 PM · Jun 29, 2022

7 Reposts **2** Quotes **27** Likes **11** Bookmarks

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

Terms of Service Privacy Policy Cookie Policy
Accessibility Ads info More ··· © 2024 X Corp.

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: https://x.com/en/privacy

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