



Settings



Post



Samir  
@SBousseaden



renamed comsvc too

[github.com/Hackndo/lsassy...](#)

[elastic.co/guide/en/secur...](#)

```
sequence by process.entity_id with maxspan=1m [process where
event.category == "process" and process.name : "rundll32.exe"]
[process where event.category == "process" and event.dataset :
"windows.sysmon_operational" and event.code == "7" and
(file.pe.original_file_name : "COMSVCS.DLL" or file.pe.imphash :
"EADBCCBB324829ACB5F2BBE87E5549A8") and /* renamed COMSVCS */
not file.name : "COMSVCS.DLL"]
```



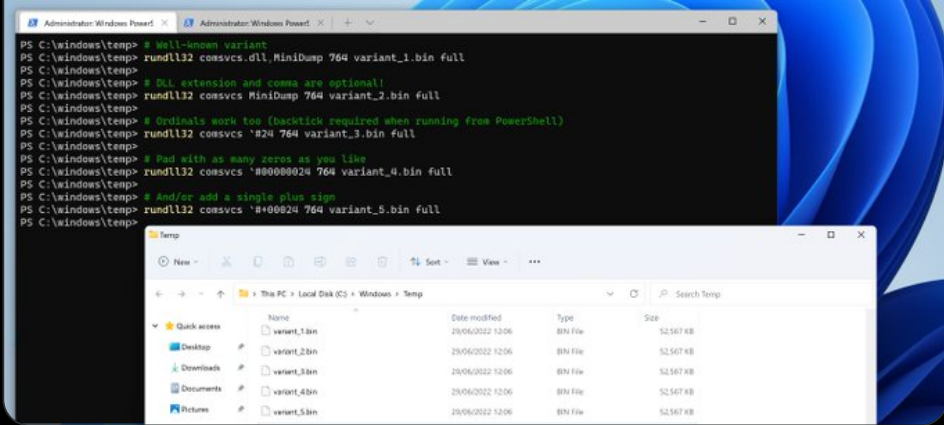
Wietze · Jun 29, 2022

#HuntingTipOfTheDay

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

...

Show more



4:33 PM · Aug 4, 2022

5 Reposts   36 Likes   7 Bookmarks



7



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