← **Post**

Samir
@SBousseaden

renamed comsvc too

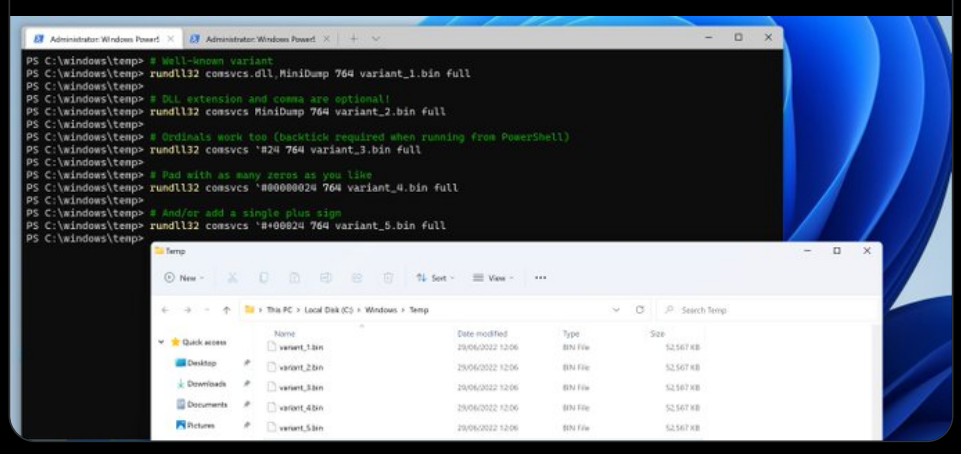
github.com/Hackndo/lsassy...

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 @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