

Forum:[Hack Forums](#)

Thread: [Can you hide your rat into PDF?](#)

Oslo - March 19, 2024, 6:35 am

Is it possible to hide rat in pdf documents? If its possible, how can be that done?

DramaKing - March 19, 2024, 6:55 am

(Mar 19, 2024 06:35 AM)Oslo Wrote: [\[CITE\]](#) Is it possible to hide rat in pdf documents? If its possible, how can be that done?

I assume that you made no attempt whatsoever to check for yourself. Try this:

<https://github.com/ratshoporg/PDF-RAT?tab=readme-ov-file>. It's probably a scam because PDFs are document files. You can still execute JavaScript in Adobe Acrobat; it will just run in a [secure sandbox](#). You might pick up something useful by browsing Google for pdf malware, or you could buy Trillium from the Marketplace.

Just to be clear, do you have Adobe Acrobat or know how few people still use it?

Binance - March 19, 2024, 5:58 pm

u cant just one click open a .pdf malware for most targs.....

however u can add a link to a direct download and social engineer ur target into installing ur .exe....

memory - March 23, 2024, 11:37 pm

(Mar 19, 2024 06:35 AM)Oslo Wrote: [\[CITE\]](#) Is it possible to hide rat in pdf documents? If its possible, how can be that done?

As others have mentioned, they are correct. You won't be able to accomplish a true .pdf filetype execution of Malware unless you stumble upon a zero day or purchase one. Even good ones are likely to still not have a true 'pdf' filetype and will just make the icon appear as a PDF and crypt it, while under the hood it is still of executable type (such as .bat, .cmd, .exe, etc)

Hackers - March 24, 2024, 8:18 am

(Mar 23, 2024 11:37 PM)memory Wrote: [\[CITE\]](#) As others have mentioned, they are correct. You won't be able to accomplish a true .pdf filetype execution of Malware unless you stumble upon a zero day or purchase one. Even good ones are likely to still not have a true 'pdf' filetype and will just make the icon appear as a PDF and crypt it, while under the hood it is still of executable type (such as .bat, .cmd, .exe, etc)

I'm assuming the wrapper func you mentioned is probably most common, or an SE method that pops open some sort of branded/custom PDF reader installer that prompts the user to install / maybe approve admin uac / etc & run the payload.