

Forum:[Hack Forums](#)

Thread: [.DOC exploit building](#)

shell33 - February 18, 2021, 7:15 am

Can anyone here help with how to use an existing CVE combined with VBA code/Macros to build malicious .DOC document? Would also need to know how to obfuscate code so it's not detected

guardian - February 18, 2021, 7:22 am

You can find all of it online. Creating a .docm backdoor is easy, making it FUD is the tricky part. If you only want .doc you will need an exploit. If there is no public code on exploit-db or the like, you will have to exploit it on your own, which is pretty hard.

zelus - February 22, 2021, 10:45 am

(Feb 18, 2021 08:22 AM)guardian Wrote: [\[CITE\]](#) You can find all of it online. Creating a .docm backdoor is easy, making it FUD is the tricky part. If you only want .doc you will need an exploit. If there is no public code on exploit-db or the like, you will have to exploit it on your own, which is pretty hard.

Do you by any chance know how to make it FUD?

hombregordo - February 26, 2021, 12:06 pm

(Feb 22, 2021 11:45 AM)zelus Wrote: [\[CITE\]](#) Do you by any chance know how to make it FUD? Google 'VBA Purging' and first page will show an article from a well known red team/ programmer with a tool on GitHub called 'OfficePurge'.

The old red team method was VBA stomping but many threat actors hv moved onto purging so this tool simulates the same attack so that companies can test it and defend themselves/update yara rules.

Many other blog posts there as well that will help you write / understand VBA, shell code , etc.

shell33 - March 1, 2021, 5:20 am

(Feb 18, 2021 08:22 AM)guardian Wrote: [\[CITE\]](#) You can find all of it online. Creating a .docm backdoor is easy, making it FUD is the tricky part. If you only want .doc you will need an exploit. If there is no public code on exploit-db or the like, you will have to exploit it on your own, which is pretty hard.

Hey thanks a lot for the very helpful reply and Instructions. Much appreciated. So you're saying to use the .docm format and use that Threat Actors page + VBA purging to make the .docm backdoor FUD?

Super - March 2, 2021, 12:29 pm

A private exe-to-doc exploit worth \$2,100 was leaked back in December 2020. It's patched now, but you can still target outdated versions of MS word.

Link: <https://github.com/bdunlap9/.Exe-to-.Doc-Exploit>

Enjoy ?

xrahitelvip - March 3, 2021, 6:30 pm

[Video: https://www.youtube.com/watch?v=atK_FmcWLcQ]

[Video: https://www.youtube.com/watch?v=9dg_aNbT3Ds]

Spidyhunt3r Offical - *March 4, 2021, 12:29 am*

im have fully fud doc builder

Sitrep - *March 5, 2021, 3:30 pm*

You have a pretty new and good guide here for that, try it out in you own lab and learn!

<https://levelup.gitconnected.com/ethical-hacking-part-13-office-macro-attacks-3a8a0cad14b7?gi=a042967f5893>