

Forum:[Hack Forums](#)

Thread: [any .doc or .jpg exploit?](#)

?Døðsky - March 29, 2016, 12:34 pm

do you guys have any .doc or .jpg exploit method?
i don't really care if its not FUD
thanks in advance

Alex Belarto - March 29, 2016, 12:51 pm

You just have to search on dedicated exploits site, like: [www\[dont\]exploit-db\[dont\]com](#)
Good Luck ?

Armada - March 29, 2016, 4:48 pm

Can not infect image files bro.

Ozgin - March 29, 2016, 5:38 pm

https://www.youtube.com/results?search_query=infect+word+files

It can be done with word and excel. It's a little sketch cuz when they open it up it says that they need to accept some mode if I recall. But With a lil social persuading. Yknow like say you wrote it on mac or an older version of word so it may be that, etc.

Armada - March 29, 2016, 5:40 pm

(Mar 29, 2016 05:38 PM)Ozgin Wrote: [\[CITE\]](#)

https://www.youtube.com/results?search_query=infect+word+files

It can be done with word and excel. It's a little sketch cuz when they open it up it says that they need to accept some mode if I recall. But With a lil social persuading. Yknow like say you wrote it on mac or an older version of word so it may be that, etc.

They have to enable and accept use of Macros, with a big fat security warning.

Not really worth it, some Silent Doc exploits in python exist, but apparently they only work up until 2010 version. I had one that supposedly worked for up till 2016, but fucked if we could get it working correctly.

Stag - March 29, 2016, 5:41 pm

When you open up the word file the user is promoted with, this document has macros would you like to enable, the macro is the exploit if they simply click no it does not work, and you can not avoid this

Armanda beat me too it ;)

Ozgin - March 29, 2016, 5:46 pm

(Mar 29, 2016 05:40 PM)Armada Wrote: [\[CITE\]](#) They have to enable and accept use of Macros, with a big fat security warning.

Not really worth it, some Silent Doc exploits in python exist, but apparently they only work up until 2010 version. I had one that supposedly worked for up till 2016, but fucked if we could get it working correctly.

mmmmm wasn't sure what it was, that is too sketch. Thanks for info!