

Forum:[Hack Forums](#)

Thread: [{TUTORIAL} Convert Exe Files Into Office Word Macro Exploits](#)

Demoralise - October 26, 2014, 5:38 pm

In this tutorial we will need these things:

Computer with Office Word
Kali Linux in VM with Metasploit
Internet Access
Your RAT server
WordPad (optional)

That is all you need :)

Steps:

1: Open Kali and scroll to this directory via Terminal. Use ls to make sure that exe2vba.rb exists:

[img]http://gxf.net/images/2014/10/26/2a76a5.png[/img]

2: Then upload your RAT to <http://ge.tt> on the PC outside the VM:

[img]http://gxf.net/images/2014/10/26/Tofix.png[/img]

3: After that, download the exe to the same directory:

[img]http://gxf.net/images/2014/10/26/41e064.png[/img]

4: Then run this command to create a vba script:

[img]http://gxf.net/images/2014/10/26/5.png[/img]

5: Followed by uploading the VBA to <http://ge.tt> , downloading it on the computer outside VM and opening the file. You want to delete all the code from the top up until the end of the PAYLOAD DATA comment:

[img]http://gxf.net/images/2014/10/26/7.png[/img]

6: By using Ctrl + A, select the rest of the text and using Ctrl + C to copy the info then Ctrl + V to paste, paste it into Word then set the colour to white:

[img]http://gxf.net/images/2014/10/26/8.png[/img]

7: Now go back to the vba, press Ctrl + Z, then Ctrl + C to copy the data. Or you could use right click - copy:

[img]http://gxf.net/images/2014/10/26/Tofix2.png[/img]

8: Now to create the macro. Take the data and do this:

[img]http://gxf.net/images/2014/10/26/9.png[/img]

9: This should open up. Click Ctrl + A then delete to erase all the info in the box and then click Ctrl + V to enter the coding from the VBA:

[img]http://gxf.net/images/2014/10/26/11.png[/img]

10: Then hit Ctrl + S, and save the file as a .docm file:

[img]http://gxf.net/images/2014/10/26/12.png[/img]

The exploit is done. Now if you send it to a victim which has their Office Word security setting set to "Disable macros with warning" and they open the file, they will get a security warning. If they allow it the file executes.

Hope you enjoy the method :)

You may have noticed my negative rep. I got repfucked recently for creating a deal dispute as a community alert by accident, a simple thread creation mistake. Omni did not like me creating a community alert to draw attention to a scam and cause unnecessary flaming so I got a repfuck. Guess I'll have to regain my rep.

Don't hesitate to post or ask questions :)

- Demoralise

Water Aura - October 26, 2014, 8:53 pm

Atleast this stops the sale of the shitty Office Word Macro Exploits which is being sold for like 200\$+.

Gr0wn - October 26, 2014, 11:38 pm

One tip OP, change the upload url. Get.t distributes their files for analysis just like virus total and dropbox. Otherwise, thanks!

dogfuker - October 26, 2014, 11:42 pm

(Oct 26, 2014 11:38 PM)Gr0wn Wrote: [\[CITE\]](#) One tip OP, change the upload url. Get.t distributes their files for analysis just like virus total and dropbox. Otherwise, thanks!

One tip, don't fucking quote the OP....

Gr0wn - October 26, 2014, 11:44 pm

(Oct 26, 2014 11:42 PM)Derby Wrote: [\[CITE\]](#) One tip, don't fucking quote the OP....

What? that was a misclick hence me editing it before your response.

OMGNEEDSLEEP - October 27, 2014, 12:56 pm

Well done, this is a pretty good tutorial and now people do not need to buy exploits.

Stephano™ - October 27, 2014, 4:03 pm

Knowing this goes for around 200\$ on the marketplace, and seeing how easy it is make me laugh ?

chuma_chums - October 27, 2014, 11:11 pm

is this all for free? it still a little too complicated for me, but instead of spending a fortune on the program to teach us. thank you man. so can anyone set it up for me using the team viewer. i will be most grateful cause i have a .exe file that i really need to convert to .doc so gmail wouldnt be able to

detect it. thanks

Demoralise - October 27, 2014, 11:15 pm

(Oct 27, 2014 11:11 PM)chuma_chums Wrote: [\[CITE\]](#) is this all for free? it still a little too complicated for me, but instead of spending a fortune on the program to teach us. thank you man. so can anyone set it up for me using the team viewer. i will be most grateful cause i have a .exe file that i really need to convert to .doc so gmail wouldnt be able to detect it. thanksThe method is old so it may be detected, Gmail still scans .docm files.

420 Blaze It - October 27, 2014, 11:16 pm

Nice, you saved lots of people some cash buying these exploits.

GenesisX86 - October 29, 2014, 3:14 am

Excellent share thanks Demoralise. Cant believe some of the haters here. lol.

Demoralise - October 29, 2014, 3:19 am

(Oct 29, 2014 03:14 AM)GenesisX Wrote: [\[CITE\]](#) Excellent share thanks Demoralise. Cant believe some of the haters here. lol.Thanks :) I really appreciate the feedback ?

Executive - November 1, 2014, 7:39 am

what macro setting is word on by default? do i have to use social engineering in order to make them change it?

Jokeh - November 1, 2014, 7:41 am

(Oct 26, 2014 08:53 PM)Water Aura Wrote: [\[CITE\]](#) Atleast this stops the sale of the shitty Office Word Macro Exploits which is being sold for like 200\$+.

I think you're refering to trickydb ;)

umberto94 - November 1, 2014, 12:07 pm

Excellent share thanks Demoralise. :)

noman1337 - November 1, 2014, 11:46 pm

thanks excellent tutorial can u upload a video tutorial

Comedic - November 2, 2014, 1:08 am

Wow this is amazing. Yea you'll just have to use a good crypter since it's pretty old , but anyways how's the output file look again? Server.doc? Something like that?

RagZorro - November 2, 2014, 1:37 am

(Nov 2, 2014 01:08 AM)Legend. Wrote: [\[CITE\]](#) Wow this is amazing. Yea you'll just have to use a good crypter since it's pretty old , but anyways how's the output file look again? Server.doc? Something like that?

If your .exe is FUD while exploit is detectable it does not make sense, because AV will catch the exploit by what the exe does not infect the victim because the doc will be moved to quarantine for example.

EXE and EXPLOIT must be FUD.

(Oct 27, 2014 11:15 PM)Demoralise Wrote: [\[CITE\]](#) The method is old so it may be detected, Gmail still scans .docm files.

Yes you are right, your method is very detectable. I wonder how many anti-virus currently detects the output file. Can you give the scan result, OP ?

If you are looking for FUD one check out my signature.

What are the benefits of FUD exploit?

You can add it as an attachment to e-mail and file will not be detectable by gmail for example.

Works on all versions of MS Office, 2013 also.

You receive ready exploit to work & support and assistance.

If you wish, I'm doing a special version that works with Java Rat as well.

It is simply not detectable. Every buyer gets a private exploit, coded from scratch so the length of FUD is much better than others.

Comedic - November 2, 2014, 1:45 am

(Nov 2, 2014 01:37 AM)RagZorro Wrote: [\[CITE\]](#) If your .exe is FUD while exploit is detectable it does not make sense, because AV will catch the exploit by what the exe does not infect the victim because the doc will be moved to quarantine for example.

EXE and EXPLOIT must be FUD.

Yes you are right, your method is very detectable. I wonder how many anti-virus currently detects the output file. Can you give the scan result, OP ?

If you are looking for FUD one check out my signature.

What are the benefits of FUD exploit?

You can add it as an attachment to e-mail and file will not be detectable by gmail for example.

Works on all versions of MS Office, 2013 also.

You receive ready exploit to work & support and assistance.

If you wish, I'm doing a special version that works with Java Rat as well.

It is simply not detectable. Every buyer gets a private exploit, coded from scratch so the length of FUD is much better than others. Oh I see. Thanks for the tip, and if I get some money some time soon, I might hit up your service

madhnrj - January 12, 2015, 8:49 pm

nice post ,thank you man ,keep posting

Last Resort - January 13, 2015, 1:08 am

Very nice tutorial. Will help me out thanks.

WorkinRoundDaClock - January 26, 2015, 11:04 am

As soon as I make my doc exploit and open it, I get an error: runtime error "13" Is there anything I can do about this?

Vaksar - January 26, 2015, 10:57 pm

Excellent detailed tutorial here.

Keep em' coming! ?

tokk - February 4, 2015, 8:08 am

thank you very nice tuto :), i going to test with my DC server

Makak - February 4, 2015, 9:51 am

Is still this working? Thanks for answer.

sspwd - February 5, 2015, 7:00 am

This is really nice... Though downloading Kali linux seem to be a pain in the ass, is too large and i can't find the setup program to run it after i downloaded. Any help would be appreciated!

tokk - February 5, 2015, 7:10 am

thank you for your tuto, he work's or not ??

Alison Wonderland - February 5, 2015, 7:13 am

(Feb 4, 2015 10:51 AM)Lugia. Wrote: [\[CITE\]](#) Is still this working? Thanks for answer.
dont think theyll remove macros from the office products
So i think it will always work

SIM-2615218 - February 14, 2015, 11:10 pm

It really worked.Thnks for this information...

Andrija - February 21, 2015, 12:34 am

Is still this working? Thanks for answer.

dadada12 - February 22, 2015, 4:59 am

Thanks man, now i know what to do, Great tutorial :)

blu3berry - February 25, 2015, 6:02 pm

Very interesting method. Is this yet FUD ?

Comedic - February 25, 2015, 6:05 pm

A very great method once again demo, haven't rat'd in years though lol. Perhaps I'll give it a look one day.

?

(Feb 25, 2015 07:02 PM)blu3berry Wrote: [\[CITE\]](#) Very interesting method. Is this yet FUD ?
I doubt it is since the method itself is obsolete.

Nalgun - March 2, 2015, 9:08 am

Nice share, these exploits are amazing thank you very much

glglgl - September 14, 2016, 10:54 am

Thank you, was looking for this :-)

O?tis - September 15, 2016, 6:51 am

(Sep 14, 2016 10:54 AM)glglgl Wrote: [\[CITE\]](#) Thank you, was looking for this :-)
10/10 Gravedig.

LastSession - September 15, 2016, 6:53 am

(Sep 14, 2016 10:54 AM)glglgl Wrote: [\[CITE\]](#) Thank you, was looking for this :-)
Does this actually still work?

kpown - September 15, 2016, 7:37 am

(Oct 26, 2014 05:38 PM)Demoralise Wrote: [\[CITE\]](#) The exploit is done. Now if you send it to a victim which has their Office Word security setting set to "Disable macros with warning" and they open the file, they will get a security warning. If they allow it the file executes.

- Demoralise

Do they HAVE to have their setting to "Disable Macros with warning"?

And is this method still FUD?

poliakov15 - *September 17, 2016, 9:24 am*

Thanks bro i very like you technique off spread 12

glglgl - *October 6, 2016, 3:24 am*

This method is not meant to be FUD. AFAIK your payload should be FUD.

citscloud - *October 6, 2016, 1:02 pm*

Nice tips, thanks for sharing...

Nice tips, thanks for sharing.....

bistro420 - *October 7, 2016, 10:15 pm*

Thanks for this Its amazing. thank you.

Ganzthe3 - *October 28, 2016, 6:13 pm*

Does this really work? Has anyone tried it yet?

majabrown - *December 25, 2016, 8:23 am*

is this tut is FUD? i try this later thanks

t0msawyer - *January 5, 2017, 8:51 pm*

thank for you tutorial and information :D