

Forum: [Hack Forums](#)

Thread: [Silent .DOC \[CVE-2015-1650 and CVE-2015-1770\]](#)

Mr. Bot - April 1, 2016, 10:49 am

Hello here is the Silent .DOC Exploit for Microsoft Office.

I share here because there is nothing private at all.

You need python to use it.

The latest works for windows XP to Windows7 + office 2007 2010 2013 and Windows 8 & Windows 8.1 + office 2007 2010

CREDIT: to Author - SILENT

link: <https://www.sendspace.com/file/4zgphw>

For pentesting purpose.

dracohacker - April 1, 2016, 10:52 pm

How can I get the code? Python code to recompile it.

Thomaz000 - April 1, 2016, 10:53 pm

Thanks ... I paid \$250 for similar and didn't work :(((((((((((((((
what is detection rate of this?

goingdownscreaming - April 2, 2016, 12:34 am

Thomaz000 -

(in linux, do this)

sha256sum aa.docm

c61de8edcaefa3518f838b0cb58ea6b33a4b86ab476aa2a5b4520e8f27ad8399

Now insert the sha string like this in a virus total url.

<https://www.virustotal.com/en/file/c61de8edcaefa3518f838b0cb58ea6b33a4b86ab476aa2a5b4520e8f27ad8399/analysis/>

If you get a hit on the link, it means someone has uploaded the file to exact file to virus total and you can get a bit of insight into the current detection rate WITHOUT uploading the file.

SHA256: c61de8edcaefa3518f838b0cb58ea6b33a4b86ab476aa2a5b4520e8f27ad8399

File name: aa.docm

Detection ratio: 8 / 56

Analysis date: 2016-04-02 04:56:26 UTC

AVware LooksLike.Macro.Downloader.a (v) 20160402

Arcabit HEUR.VBA.Trojan.e 20160402

Avast VBA:Downloader-MA [Trj] 20160402
Fortinet WM/Agent!tr 20160401
McAfee W97M/Downloader.aar 20160402
McAfee-GW-Edition W97M/Downloader.aar 20160402
NANO-Antivirus Trojan.Script.Agent.drfzeu 20160402
VIPRE LooksLike.Macro.Downloader.a (v) 20160402

Ontop of this. take the SHA256 string and throw it into google and here is what you get.

<https://www.hybrid-analysis.com/sample/c61de8edcaefa3518f838b0cb58ea6b33a4b86ab476aa2a5b4520e8f27ad8399?environmentId=1>

Mr_Bot - April 2, 2016, 4:27 am

@thomaz000

Sorry for you hope you will like it ;)

QU?CKSILVER - April 2, 2016, 3:15 pm

1. The file within the rar file is a macro enabled document.
2. This is not a silent exploit
3. We're not dumb, we will not enable macros. It will obviously download and execute somebody's payload.

OP updated download link to the proper content.

Thanks for the contribution. Appreciate it ?

Mr_Bot - April 2, 2016, 4:40 pm

@DPjunisher

Check it bro should be fine now :)

I was uploading a sample found on web which was wrong sorry.

QU?CKSILVER - April 2, 2016, 4:50 pm

(Apr 2, 2016 04:40 PM)DigitStudio Wrote: [\[CITE\]](#) @DPjunisher

Check it bro should be fine now :)

Yup, just checked the file, it contains a .py file with the code in it.

Thank you for that. Does it work on MSOffice 2013?

Mr_Bot - April 2, 2016, 4:54 pm

I didn't coded that or use it myself.

But as you see

Quote: works for windows XP to Windows7 + office 2007 2010 2013 and Windows 8 & Windows 8.1 + office 2007 2010

Then yea he work if is Windows 7 or less.