

Forum:[Hack Forums](#)

Thread: [The Rise of PDF Malware | How do I prevent getting infected by a PDF file?](#)

Zoomer - February 17, 2018, 5:36 am

Hello,

I love reading ebooks and it's becoming a real problem nowadays where I don't dare to open ebooks anymore, a lot threads here on hackforums that sell products nearly includes free pdf exploits and what not. making this the era of pdf malware.

Now i'm not a hacker at all, but I would like to know how to protect myself from getting infected by PDF files.

So that's pretty much my question, How do i prevent getting infected by a PDF file & How do i know a PDF file is infected?

Appreciate any help i can get with this.

Vyxn - February 17, 2018, 7:01 am

Good day sir.

Everyday, malware was becoming sophisticated just to enter into our machines. Nothing is an absolute protection, every corner has a flaws.

The best protection was your only self.

Here's some of my tips:Install an antimalware

- My recommendation was [MalwareBytes](#). It is best known for their up to date database and fighting against Oday.

Scan the pdf.

- You can scan it and some of the antimalware software can pick up some malicious code on it.

- You can also use a free tools online like [Virusotal](#) or [Hybrid Analysis](#)

Always read about vulnerabilities of the software like Adobe Reader or Google Chrome (you can read pdf on it).

Always stay your operating system/antimalware up to date.

Hope it will gives you an idea on how to be protected. Not an absolute tips but this will do for now.
?

Zoomer - February 17, 2018, 10:07 am

First of all thank you for the comment, it's much appreciated.

But everyone here on hackforums is offering PDF exploits that bypass Malwarebytes or other Antivirus programs. Now I understand it's always good to run Antivirus programs to protect you as much as possible.

Is there a way to run PDF files on sandboxie? That way when you open the PDF file you can see whether a virus is embedded.

Again i'm not a hacker or have any knowledge but there must be a way to open the file and see if

anything tries to secretly install itself onto the machine.

Barb - February 17, 2018, 10:13 am

Majority of the time the exploit is most likely with the software opening the PDF than the file itself, use something other than Adobe products and you should more than likely be in the clear.

Play Boy - February 17, 2018, 10:38 am

You can open the file on a virtual machine to observe how it behaves as well. Look for creation of files, opening of ports, or unknown/unnecessary services running. The difficult part comes into play when dealing with skilled malware writers as it becomes difficult to detect abnormal behavior.

CyberStrike - February 17, 2018, 11:27 am

PDF's have been a vector for infection for a very long time. Either way I tend to analyze the pdfs using pdfid/pdf-parser/pdfinfo. But if you are not into this stuff then as suggested use AV.

Vyxn - February 17, 2018, 4:35 pm

(Feb 17, 2018 11:07 AM)Zoomer Wrote: [\[CITE\]](#) First of all thank you for the comment, it's much appreciated.

But everyone here on hackforums is offering PDF exploits that bypass Malwarebytes or other Antivirus programs. Now I understand it's always good to run Antivirus programs to protect you as much as possible.

Is there a way to run PDF files on sandboxie? That way when you open the PDF file you can see whether a virus is embedded.

Again i'm not a hacker or have any knowledge but there must be a way to open the file and see if anything tries to secretly install itself onto the machine.

I haven't recommended a virtual machine as I don't see it used by a normal users.

For the sandboxie part, you can open Google Chrome in Sandboxie then drag and drop your pdf file there. I don't know if you can able to run the adobe reader on the sandboxie.

PerfectStorm - February 17, 2018, 4:38 pm

I second the virtualmachine it seems pretty obvious to me.

Zoomer - February 18, 2018, 2:21 am

Thanks for everyones input, i'll use the virtualmachine to be on the sure side of things.

ColeBot - February 18, 2018, 7:56 am

(Feb 17, 2018 06:36 AM)Zoomer Wrote: [\[CITE\]](#) Hello,

I love reading ebooks and it's becomming a real problem nowadays where I don't dare to open ebooks anymore, a lot threads here on hackforums that sell products nearly includes free pdf exploits and what not. making this the era of pdf malware.

Now i'm not a hacker at all, but I would like to know how to protect myself from getting infected by PDF files.

So that's pretty much my question, How do i prevent getting infected by a PDF file & How do i know a PDF file is infected?

Appreciate any help i can get with this.

Open all pdf files in a VM or possibly do a scan on them first.

SysAdmin - February 18, 2018, 8:17 am

I'm fairly surprised that nobody (Except one guy) pointed out that these actually bypass Anti-Virus and Anti-Malware software. The best thing to do would still be opening it up in a VM and seeing it's behaviour, what it drops, what packets it sends and to who when executed, etc..

Zoomer - February 18, 2018, 8:31 am

(Feb 18, 2018 09:17 AM)SysAdmin Wrote: [\[CITE\]](#) I'm fairly surprised that nobody (Except one guy) pointed out that these actually bypass Anti-Virus and Anti-Malware software. The best thing to do would still be opening it up in a VM and seeing it's behaviour, what it drops, what packets it sends and to who when executed, etc..

It's scary how advanced things have become, people who are unaware or don't have a clue about this to begin with are so screwed.

Does the average person even know what a Virtual machine is or finding out whether it is or isn't infected..

I'm giving up on PDF's until things become regulated.

SysAdmin - February 18, 2018, 11:42 pm

(Feb 18, 2018 03:41 PM)Disparity Wrote: [\[CITE\]](#) you're fucking retarded

you're fucking retarded

you're fucking retarded

you're fucking retarded

PDFs aren't vulnerable. That's not how it works.

Keep your PDF reader up to date and you won't get infected. If you're that paranoid use sandboxie as someone else suggested, but you don't need to. And yes, sandboxie or any other sandbox program will work with your pdf reader.

Funny how you call everyone retarded but fail to realise that nothing is 100% secure, even up to date PDF Readers can work with the very same exploits, or if they get patched, new ones are being found daily.

I don't think it's worth pointing out that .pdf files are not vulnerable, but the readers for it are. Not everyone updates to the latest version when it comes out, as most people find it annoying, time consuming and not worth their time. If people did update everything, Penetration Testers wouldn't have a job.

Disparity - February 19, 2018, 12:49 am

(Feb 19, 2018 12:42 AM)SysAdmin Wrote: [\[CITE\]](#) Funny how you call everyone retarded but fail to realise that nothing is 100% secure, even up to date PDF Readers can work with the very same exploits, or if they get patched, new ones are being found daily.

I don't think it's worth pointing out that .pdf files are not vulnerable, but the readers for it are. Not everyone updates to the latest version when it comes out, as most people find it annoying, time consuming and not worth their time. If people did update everything, Penetration Testers wouldn't have a job.

I see. So you're not only retarded, but lack reading comprehension.

(Feb 19, 2018 12:42 AM)SysAdmin Wrote: [\[CITE\]](#) Funny how you call everyone retarded but fail to

realise that nothing is 100% secure, even up to date PDF Readers can work with the very same exploits, or if they get patched, new ones are being found daily.

Very good point. You know, I think I'm going to stop using my web browser, actually. Actually, I'm going to stop using my OS. Nothing is 100% secure, afterall. Both Firefox and Windows have had exploits found... what if I run into a 0day jdb?!?!?! Even up to date browsers and can be vulnerable to the very same exploits!!! The only way I can survive is by being paranoid because I think I know what I'm talking about but don't and run every PDF file I run into in a VM and monitor the OS for anything weird.

(Feb 19, 2018 12:42 AM)SysAdmin Wrote: [\[CITE\]](#) I don't think it's worth pointing out that .pdf files are not vulnerable, but the readers for it are. Not everyone updates to the latest version when it comes out, as most people find it annoying, time consuming and not worth their time. If people did update everything, Penetration Testers wouldn't have a job.

Then follow my advice and update. Did you just skip the part of my post that wasn't flame?

You recommend that people setup a vm and monitor what every pdf does yet you claim you're not retarded. ???

Zoomer - February 19, 2018, 4:15 am

C'mon guys that's not nice, everyone here is trying to share their opinion and advice on how to be more secure. There's no need to belittle eachother over who knows best, everyone gave useful and helpful advice in this thread.