

Forum:[Hack Forums](#)

Thread: [Python - PNG Payload FUD - Say What?](#)

antipriced - December 4, 2022, 7:56 pm

Above is a PNG image of a T-Rex. nothing to worry about right?

Virus total says its safe, so does norton, malwarebytes and every other program that we are told to depend on

BUT WHAT if that trex was actually a keylogger or ransomware or stealer or WHAT IF IT automated something good? hidden deep in the dark pixels of obfuscation nation??

Please note for the sake of this tutorial it actually is just an image for visual pleasure only. I will now teach you how to actually make a image containing a payload that indeed fools all these false security providers and can execute code from a remote location OH SNAP, lets get started shall we?

We are going to need a few essential things to make this happen, nothing costs money - so your good to go brokeski.Computer

Python installed

github or other raw text hosting on the big WWW

some png image of your choice

something naughty or nice in python code (.py) your wanting to FUD

understanding that this tutorial is not intended for illegal use and is only for educational purposes.

LETS GOOO!

Begin by making a folder to store all this in on your computer, for the tutorial my folder is called "HOMEFOLDER"

navigate into this folder and create "thecode.py" "thepayload.txt" as files, and add you "Image.png" should look like this

HOMEFOLDERthecode.py

thepayload.txt

Image.png

? Time

right click on thecode.py and open in notepad (or your favorite text editor its 2022 no judgement)
add the following code to it:

[code](#)

once your done that paste the following code directly below it in the same thecode.py file:

[second half of code](#)

save thecode.py

note if you did it right to this point, executing will return this

Code Image Payload Kit - AntiPriced

Build Payload (1) or execute (2) ?

next we need to host the payload nonsense: for this tutorial im going to keep it clean and use this
as a payload

Code print("antipriced hackforums ")

print("it worked")

save it to github and get the raw link (click view raw)

ok just for the plebs :

"https://raw.githubusercontent.com/YOUR ACCOUNT / YOUR REPO /main/THEPAYLOAD.text"

now running the code.py that you made:

choose option 1

Code Image Payload Kit - AntiPriced

Build Payload (1) or execute (2) ?

> 1

PROTIP :

Payload must be python code

hosted on a url in raw format

Enter url to raw data of payload :insert your link at this point and notice that a new image has been
added to your "HOMEFOLDER" called "EVIL.PNG"

Code New picture saved as 'EVIL.png'!

Thats it! Your PNG payload is ready for action.

wait what happened?

the new image is encoded with a link to your harmless raw text link.

now what?

Im not sure about the rules on explaining the execution of option 2 but the codes there to examine
how it will remotely download the code make the target create the actual payload and launch the
payload and delete all its traces.

I wrote the code, and the guide, I'm looking forward to your feedback.

nietdoen - January 26, 2023, 4:47 am

must the made up target also have python on his pc?

antipriced - January 27, 2023, 3:01 pm

(Jan 26, 2023 05:47 AM)nietdoen Wrote: [CITEI](#) must the made up target also have python on his
pc?

python is a standard part of most os these days, but to be more clear, everything would matter on

what you choose to put into your image, if that is a concern for you, there is powershell / bash coding you can use to ensure they have python.

NiNJAA - January 30, 2023, 7:44 am

not work for me you have any video ?

antipriced - January 30, 2023, 7:57 am

(Jan 30, 2023 08:44 AM)NINJA.b0x Wrote: [\[CITE\]](#) not work for me you have any video ?

works

NiNJAA - January 30, 2023, 6:02 pm

(Jan 30, 2023 08:57 AM)antipriced Wrote: [\[CITE\]](#)

works

possible to .exe excute via png ?

antipriced - January 30, 2023, 11:06 pm

(Jan 30, 2023 07:02 PM)NINJA.b0x Wrote: [\[CITE\]](#) possible to .exe excute via png ?

The entire purpose of this is the have the payload go undetected, thus sending a packed executable would not be smart or effective. the fundamental purpose is the target will unknowing download source code, compile it launch it and delete it before they know they did it, this works because the commands appear to come from the end target building the payload locally and not being scanned on the way in as an flagged exe for example.

NiNJAA - January 30, 2023, 11:46 pm

(Jan 31, 2023 12:06 AM)antipriced Wrote: [\[CITE\]](#) The entire purpose of this is the have the payload go undetected, thus sending a packed executable would not be smart or effective. the fundamental purpose is the target will unknowing download source code, compile it launch it and delete it before they know they did it, this works because the commands appear to come from the end target building the payload locally and not being scanned on the way in as an flagged exe for example.

OOOH OK thanks can you give me your code ? this one not work me dont know why which python version used ?

The_unknown - January 31, 2023, 9:00 am

Hi thank you for ths great tutorial. When I try it at first there were some problems with the import but after that it worke perfect. This tutorial is one of the best free payload tutorials I have seen.

antipriced - January 31, 2023, 11:21 am

(Jan 31, 2023 10:00 AM)The_unknown Wrote: [\[CITE\]](#) Hi thank you for ths great tutorial. When I try it at first there were some problems with the import but after that it worke perfect. This tutorial is one of the best free payload tutorials I have seen.

Thx for your feedback, glad to help