

Forum:[Hack Forums](#)

Thread: [How To Bind My Rat Exe File Into A Picture Jpg File](#)

Bro codes - September 27, 2019, 6:23 pm

Hey, im just wondering if there is any easy ways to hide my rat in a Picture file? have tried a few Methods, but none did work. Well i was able to hide the file into a Picture, but it wouldnt run the exe when the Picture was opened.

Kryme - September 27, 2019, 6:31 pm

Seems way too hard. However binding to a .scr

Now that's a different story ?

?mazon - September 27, 2019, 7:17 pm

(Sep 27, 2019 06:31 PM)Kryme Wrote: [\[CITE\]](#) Seems way too hard. However binding to a .scr

Now that's a different story ?

Don't think anyone uses a screensaver anymore (like downloads them). :shrug:

Kryme - September 27, 2019, 7:20 pm

(Sep 27, 2019 07:17 PM)Lorikeet Wrote: [\[CITE\]](#) Don't think anyone uses a screensaver anymore (like downloads them). :shrug:

Just add it among other files in an .rar file, people tend to click on the .scr without a second thought if it is surrounded with 5-10 other files

?mazon - September 27, 2019, 7:21 pm

(Sep 27, 2019 07:20 PM)Kryme Wrote: [\[CITE\]](#) Just add it among other files in an .rar file, people tend to click on the .scr without a second thought if it is surrounded with 5-10 other files

That's true, its all about social engineering how your payload looks like.

Noshy - September 28, 2019, 2:46 am

you can bind your exe with img file with any binder but the output will be .exe

zetoid - September 28, 2019, 5:42 pm

Hey, just use any binder!

CyberStrike - September 28, 2019, 6:12 pm

There are many executable files. this whole let's bind an exe to a jpg is silly, when you are able to use already proven methods in polyglot images. A good search would help as this has been discussed so much already.

HackersI - September 29, 2019, 1:30 am

Me too tried.I could bind .exe .

But I couldnt bind payload.apk file.

CyberStrike - September 29, 2019, 1:40 am

(Sep 29, 2019 01:30 AM)HackersI Wrote: [\[CITE\]](#) Me too tried.I could bind .exe .

But I couldnt bind payload.apk file.

You tried to bind an exe to an APK?

HackersI - September 29, 2019, 8:47 am

(Sep 29, 2019 01:40 AM)CyberStrike Wrote: [\[CITE\]](#) You tried to bind an exe to an APK?

Ohhhh nop.

Apk to jpg or pig

Claw - September 29, 2019, 10:54 am

What are you guys talking about, exe to jpg, exe to apk, like seriously?, jpeg exploits are hard to get or even i might say it doesn't exist imo, and exe to apk, meh don't even try.

CyberStrike - September 29, 2019, 11:48 am

(Sep 29, 2019 08:47 AM)HackersI Wrote: [\[CITE\]](#) Ohhhh nop.

Apk to jpg or pig

Are jpeg's or jpg file types polyglot? You can bind an APK to a PNG I know that happens. (PNG != Papua New Guinea)

(Sep 29, 2019 10:54 AM)Illusion Wrote: [\[CITE\]](#) What are you guys talking about, exe to jpg, exe to apk, like seriously?, jpeg exploits are hard to get or even i might say it doesn't exist imo, and exe to apk, meh don't even try.

It's the equivalent of hacking masturbation to bind an executable with a jpg, at least for some circles. The jpeg is what is odd, they can bind APK's and executables with polyglot images, there are jpg polyglot's but not in the way that is expected here in this discussion.

Claw - September 29, 2019, 2:40 pm

(Sep 29, 2019 11:48 AM)CyberStrike Wrote: [\[CITE\]](#) Are jpeg's or jpg file types polyglot? You can bind an APK to a PNG I know that happens. (PNG != Papua New Guinea)

It's the equivalent of hacking masturbation to bind an executable with a jpg, at least for some circles. The jpeg is what is odd, they can bind APK's and executables with polyglot images, there are jpg polyglot's but not in the way that is expected here in this discussion. Mate, no one wants only speeches, imo jpeg exploits doesn't exist nor exe to apk.

CyberStrike - September 29, 2019, 2:52 pm

(Sep 29, 2019 02:40 PM)Illusion Wrote: [\[CITE\]](#) Mate, no one wants only speeches, imo jpeg exploits doesn't exist nor exe to apk.

You're thinking exploit I am saying something different polyglot. Also I am not saying jpeg although there is one such payload I know of.

Racquelialicia6 - October 12, 2019, 8:10 am

If you want the file to have a genuine file extension of a picture file format like *.jpg then you will need to identify a vulnerability in a graphic software that you can exploit for arbitrary code execution and weaponize to get your image ran from memory by the affected process (which in this case would be Microsoft Paint, Microsoft Photos UWP application, etc.).

However, you would be assuming that the user of the system will be using the same software you have exploited to open the image up.

If you already have code execution on the target machine then you can use any extension you want on the file and then have it executed as long as it is identified as executable by the PE file header markers (e.g. MZ bytes at the start of the binary) or a manual loader for it.

Your best bet would be exploiting the human mind: make the file appear to be an image and open up a genuine image on execution, but really it would be executable in some shape or form. There

are many tricks that can be played with archive formats and Java as well.

nameless_cro1 - *December 4, 2019, 8:20 am*

Im looking for same solution, and like 8-9 years ago it existed.

I was able to hide .exe into .jpg,

when someone clicks on it it opens picture while rat installs in background.

Only minus was that in name of jpg was always .exe,

so my picture was named/looked like this: Latexe.jpg

thegardner - *December 4, 2019, 12:04 pm*

So, please correct me if I'm wrong. But if you wanted to spend some money, couldn't you get a crypter with a file binder?