

Forum:[Hack Forums](#)

Thread: [Why do AV's Detect .scr Extensions](#)

Surge0n - May 24, 2017, 11:09 am

If I execute a malware as .exe, it would bypass but once renamed to .scr, the AV wont allow any chance for execution and would delete it instantly as "Trojan Generic" whether file is runtime FUD or not. But then when a legit program is changed to .scr, it was allowed to run.

Any workaround here?

EDIT: Pls I still need help with this. I thought cloning a legit app's assembly solved this but it didn't.

HOLLOWZ - May 24, 2017, 3:30 pm

Well not sure if this relates but one time I used a crypter on my .exe which was FUD then used a binder to bind with a clean software and it came out fully infected could be the same type issue not sure though

Surge0n - May 24, 2017, 3:36 pm

(May 24, 2017 03:30 PM)HOLLOWZ Wrote: [\[CITE\]](#) Well not sure if this relates but one time I used a crypter on my .exe which was FUD then used a binder to bind with a clean software and it came out fully infected could be the same type issue not sure though

Yes binders are detected af; always bind before you crypt.

Then again you're right, it's unrelated to my issue rn.

.exe bypasses but .scr won't bypass whether fud or not

HOLLOWZ - May 24, 2017, 3:41 pm

I used this one program called spooov has many functions even for extensions try search n see if it will work for you the few time I used it didn't have an issue file was still FUD and executed

Surge0n - May 24, 2017, 3:53 pm

(May 24, 2017 03:41 PM)HOLLOWZ Wrote: [\[CITE\]](#) I used this one program called spooov has many functions even for extensions try search n see if it will work for you the few time I used it didn't have an issue file was still FUD and executed

Can you please install an AV, 360 to be specific; then rename your exe payload to .scr and try to run it. Then Lmk what you got pls

I still need info on this @everyone

HOLLOWZ - May 24, 2017, 3:58 pm

Shiit das mad work rn lol on my phone in my bed

occupi - May 24, 2017, 3:59 pm

.scr files are executables too so they've been suspicious af for a long time now. If your software isn't signed I doubt you'll succeed imitating a .scr file in 2017.

yotoprules - May 25, 2017, 11:25 pm

(May 24, 2017 03:36 PM)Surge0n Wrote: [\[CITE\]](#) Yes binders are detected af; always bind before you crypt.

Then again you're right, it's unrelated to my issue rn.

.exe bypasses but .scr won't bypass whether fud or not
NEVER bind before you crypt. Just bind the files yourself or use an FUD binder. They're not hard to find?

Purple Kief - May 26, 2017, 7:13 am

Antivirus's don't detect .scr files as malicious lol.

I can already see the mass amount of screenshots with .scr extension get flagged.

?Criminal - May 26, 2017, 4:29 pm

Try to make a .scr downloader those usually aren't flagged.

Surge0n - May 27, 2017, 5:45 am

(May 26, 2017 07:13 AM)Purple Kief Wrote: [\[CITE\]](#) Antivirus's don't detect .scr files as malicious lol.

I can already see the mass amount of screenshots with .scr extension get flagged.

But you're wrong, 360 does or maybe it's only 360.

If you rename a signed program to scr, it won't detect it. But any other unsigned exe (both malicious and harmless) that you rename to scr gets flagged and won't execute

(May 26, 2017 04:29 PM)?Criminal Wrote: [\[CITE\]](#) Try to make a .scr downloader those usually aren't flagged.

Tried with that already. Same shit, I think all it checks is if it's signed or not

Purple Kief - May 27, 2017, 2:42 pm

(May 27, 2017 05:45 AM)Surge0n Wrote: [\[CITE\]](#) But you're wrong, 360 does or maybe it's only 360.

If you rename a signed program to scr, it won't detect it. But any other unsigned exe (both malicious and harmless) that you rename to scr gets flagged and won't execute

You seem to forget that the .scr extension does not belong to any programs.

It belongs to screenshots only.

If I was an antivirus program, I'd flag the shit out of anything that's supposed to be an executable but has the .scr extension and is unsigned.

It's not the .scr extension, it's that + an unsigned executable that trigger the detection.

Obviously if you rename Teamviewer to TV.scr it won't get flagged, the AV will read the signature and recognise it as a legit program.

If you think about it it's rather clever by the 360 crew. ?

5chn4pp - May 27, 2017, 3:06 pm

.scr malware files usually contains ransomware, ofc this is not the case with all .scr files.

(May 27, 2017 05:45 AM)Surge0n Wrote: [\[CITE\]](#) But you're wrong, 360 does or maybe it's only 360.

If you rename a signed program to scr, it won't detect it. But any other unsigned exe (both malicious and harmless) that you rename to scr gets flagged and won't execute

That Chinese marketing antivirus shit will detect everything