

Forum:[Hack Forums](#)

Thread: [RAT in .Dll inject](#)

odesey - August 20, 2021, 12:49 am

Hi all.

Who is familiar with such a problem and can help me?

I have a self-written RAT.dll, on github I found dllinjector.c / .exe

How can I make one program out of these two programs so that when I start my RAT.dll is automatically added to kernel32.dll?

This can be done?

SIM-5063966 - August 20, 2021, 3:54 am

Hi!

You can "host" your rat.dll on discord, upload it in a conv. with a friend / bot and copy the direct download link. Edit your dllinjector.c and make it download the file from your direct link, then inject the dll into kernel. I don't know if you can somehow merge the dll with the exe, but atleast you can download it into appdata/temp (locations that don't require administrator privileges) and then inject it.

rekted - August 20, 2021, 9:37 am

why you can't just use RunPE? or inject dll to some legit process, maybe discord.exe?

Sajuuk - August 20, 2021, 10:54 am

(Aug 20, 2021 03:54 AM)WtfIsThis Wrote: [\[CITE\]](#) Hi!

You can "host" your rat.dll on discord, upload it in a conv. with a friend / bot and copy the direct download link. Edit your dllinjector.c and make it download the file from your direct link, then inject the dll into kernel. I don't know if you can somehow merge the dll with the exe, but atleast you can download it into appdata/temp (locations that don't require administrator privileges) and then inject it.

Even if it's a couple kilobytes, that network activity will likely be seen as suspicious by every semi-decent AV.

odesey - August 20, 2021, 11:26 am

I want my malware code to be automatically added to kernel32.dll when I run my rat.exe

SIM-5063966 - August 20, 2021, 11:31 am

(Aug 20, 2021 10:54 AM)Sajuuk Wrote: [\[CITE\]](#) Even if it's a couple kilobytes, that network activity will likely be seen as suspicious by every semi-decent AV.

I don't really know, there are a lot of FUD droppers.

Sajuuk - August 20, 2021, 11:57 am

(Aug 20, 2021 11:31 AM)WtfIsThis Wrote: [\[CITE\]](#) I don't really know, there are a lot of FUD droppers.

Well, I guess try it. If it works, stick with it.