

Forum:[Hack Forums](#)

Thread: [Add C:\ partition for any AntiVirus exclusions](#)

aerohacker - November 28, 2024, 10:34 pm

The feature to add C:\ partition in Windows Defender exclusions is very common in some RATs and Crypters and can be done with programs and scripts too, but there's a way to do the same for other AntiVirus?!

I think the best way to do that would be using HVNC or HRDP, open the AntiVirus and add manually C:\ partition to exclusions, in case that a lot of users, it would be nice to do this automatically.

Bastille - November 29, 2024, 12:16 am

Manually you can do it, with a GUI, however if the hacker wants to remain stealthy he should use the CLI.

For for the CLI that's not that simple if you plan to add the exclusion path during the execution of the payload, as you don't know which antivirus the victim has on his computer, and the command used will be different, except if you implement the commands for the most used antivirus. If you already have a remote access to the computer then it could be easier, but for a initial compromission it's a little bit tricky I think.

However, it seems that CLI options are not available for many antivirus that are sold to individuals, but the CLI commands are available for profesionnal products, but profesionnal products are usually protected by admin or tempered passwords, so if you plan to use the CLI option you'll be asked to use a password to unlock the antivirus to make the modifications.

DramaKing - November 29, 2024, 4:10 am

(Nov 28, 2024 11:34 PM)aerohacker Wrote: [\[CITE\]](#) The feature to add C:\ partition in Windows Defender exclusions is very common in some RATs and Crypters and can be done with programs and scripts too, but there's a way to do the same for other AntiVirus?!

I think the best way to do that would be using HVNC or HRDP, open the AntiVirus and add manually C:\ partition to exclusions, in case that a lot of users, it would be nice to do this automatically.

Most antivirus do not have CLI like Bastille mentioned because it's idiotic. Any control of the antivirus is shielded and restricted. HVNC requires avoiding detection to start with, so you would only be able to disable AV for a later stage infection. EDR/XDR isn't going to have any GUI to whitelist or exclude anything. Plus, any antivirus commands that do exist will require admin.