

# Forum:[Hack Forums](#)

Thread: [Windows Defender Exclusions](#)

**RoadLess** - February 22, 2023, 12:32 pm

Hey, I've seen that many crypters add C:\users folders to windows D exclusions. Is C\Users really needed or just C\ or do you have other ideas?

**Ph4n70M Phr34K** - February 23, 2023, 1:24 am

c drive or most used locations such as temp/appdata  
same for file types for example .exe

**blyat1337** - February 23, 2023, 11:45 am

Exclusions are per file or folder, it doesn't matter. Usually you exclude a folder because it is easier to maintain.

**RoadLess** - February 27, 2023, 10:31 am

(Feb 23, 2023 12:51 PM)Dyne Wrote: [\[CITE\]](#) Keep in mind this will significantly ruin your results with other antivirus.

Though WD's portion of the market segment is huge, avast free for example will immediately flag and quarantine your file if it detects a .bat script or something like a metasploit output is attempting to disable WD or alter exclusions.

C: is fine for most purposes, but %temp% or %AppData% flags less. Most loaders drop here anyway.

I only used the C folder. When scanning 1/27 by malwarebytes (ldk is it false positive). Kleenscan all FUD. Will test other folders and see if it improves detection.

**RoadLess** - February 27, 2023, 10:56 am

(Feb 27, 2023 11:42 AM)Dyne Wrote: [\[CITE\]](#) Hello,

Now, as part of your RUNTIME test(kleenscan, Avcheck etc only check scantime. There is a huge difference), install avast free on a virtual machine and run your malware that adds c: to exclusions on WD.

When another antivirus is running, and permissions over WD, any exclusions to WD attempted will flag your file immediately.

You will literally see a window that says "Malware has attempted to make alterations to Windows Defender!"

So, it doesn't matter if it comes up clean vs other AVs.

Though this is a good test against WD which 80% of the worlds' population runs, it will literally destroy your chances vs other antivirus.  
Just be warned in this respect.

Bruh, I tested on VmWare Windows 10. Windows Defender did not detect viruses when downloading, extracting and running. I obfuscated the file and it seems to me that the antivirus is unable to read the script. Windows Defender itself was bypassed and avast, avg and the rest of the popular avs I checked on RunTimeCheck on a kleenScan where no threads were found either.

I can record a video of how I run a file on a new machine without additional exclusions in WD.

**scanbuddy** - February 28, 2023, 9:14 am

(Feb 27, 2023 11:56 AM)RoadLess Wrote: [\[CITE\]](#) Bruh, I tested on VmWare Windows 10. Windows Defender did not detect viruses when downloading, extracting and running. I obfuscated the file and it seems to me that the antivirus is unable to read the script. Windows Defender itself was bypassed and avast, avg and the rest of the popular avs I checked on RunTimeCheck on a KleanScan where no threads were found either.

I can record a video of how I run a file on a new machine without additional exclusions in WD.  
To get most accurate results, do a runtime scan with interent ON at scanner.to.  
Send me your username in priv and I will give you 10 free scan tokens.

**RoadLess** - February 28, 2023, 11:53 am

(Feb 28, 2023 10:14 AM)scanbuddy Wrote: [\[CITE\]](#) To get most accurate results, do a runtime scan with interent ON at scanner.to.  
Send me your username in priv and I will give you 10 free scan tokens.

I've never heard of scanner.to. I'll send it to you when I create an account.

**\_\_Digital\_\_** - February 28, 2023, 12:15 pm

(Feb 28, 2023 10:14 AM)scanbuddy Wrote: [\[CITE\]](#) To get most accurate results, do a runtime scan with interent ON at scanner.to.  
Send me your username in priv and I will give you 10 free scan tokens.  
The main question is do you have api and or bigger plans for developers ?

**scanbuddy** - February 28, 2023, 2:17 pm

(Feb 28, 2023 01:15 PM)\_\_Digital\_\_ Wrote: [\[CITE\]](#) The main question is do you have api and or bigger plans for developers ?  
Bigger plans yes. API not yet.