

Forum: [Hack Forums](#)

Thread: [Add C:\ to AntiVirus exclusions is enough?!](#)

aerohacker - May 3, 2026, 9:27 am

Once you've gained access to a PC and ensured persistence, what do you usually do to maintain persistence for as long as possible?!

- Add C:\ to the AntiVirus exclusions is enough or some module can one time or another detect the RAT server?!
- Uninstall the AntiVirus would be ideal, but this could generate suspicion.

DramaKing - May 3, 2026, 10:20 am

So you're back with another highly intelligent post.

Excluding top-level directories is not always enough.

You have virtually no way to create exclusions without physical access.

You have as much chance of doing this as #2.

aerohacker - May 3, 2026, 2:11 pm

And here we go again...

And you with these "intelligent", stupid sarcams and superficial answers... from someone who doesn't see beyond and doesn't think outside the box!

1 - That's exactly why uninstall any security solution would be ideal, whether it's AV/EDR... but even the most lay user may notice that something is missing or at one time or another he or another more experienced user needs or wants to open or run an AntiVirus scan, so adding C:\ to the exceptions, would be a less suspicious option.

2 - Have you ever used HVNC or HRDP?!

3 - Another options would be install a legitim Remote Desktop tool, just in case the server would be detected and have a way to come back or Kernel Rootkit or Bootkit, that works on same AntiVirus level or start before Operating System, to keep FUD and the server persistent.

Understand one thing, when I ask questions, it's not just to clear up doubts, because as you yourself saw, I know what to do, but it's important to keep an open mind, read, see and think about other alternatives, this is called feedback.

When someone asks things like "which Operating System, AntiVirus, RAT, Crypter or another software is better?!" or which one do you use and why?!

It is not always a matter of doubt, but wanting to know the reason, pros and cons, and deeper answers of why someone prefers to use this than that.

DramaKing - May 3, 2026, 4:27 pm

(May 3, 2026 02:11 PM)aerohacker Wrote: [\[CITE\]](#) And here we go again...

And you with these "intelligent", stupid sarcams and superficial answers... from someone who doesn't see beyond and doesn't think outside the box!

1 - That's exactly why uninstall any security solution would be ideal, whether it's AV/EDR... but even the most lay user may notice that something is missing or at one time or another he or another more experienced user needs or wants to open or run an AntiVirus scan, so adding C:\ to the exceptions, would be a less suspicious option.

2 - Have you ever used HVNC or HRDP?!

3 - Another options would be install a legitim Remote Desktop tool, just in case the server would be detected and have a way to come back or Kernel Rootkit or Bootkit, that works on same AntiVirus level or start before Operating System, to keep FUD and the server persistent.

Understand one thing, when I ask questions, it's not just to clear up doubts, because as you yourself saw, I know what to do, but it's important to keep an open mind, read, see and think about other alternatives, this is called feedback.

When someone asks things like "which Operating System, AntiVirus, RAT, Crypter or another software is better?!" or which one do you use and why?!

It is not always a matter of doubt, but wanting to know the reason, pros and cons, and deeper answers of why someone prefers to use this than that.

Superficial? I'll take that. Stupid? Compared to whom?

If it was as easy as uninstalling AV, AV would be worthless, blackhats would rule the interwebs, and the Internet would be too dangerous to use. Try uninstalling any AV on your own PC. AV developers make it a special kind of difficult even when you're sitting at the machine. EDR cannot be uninstalled by users. Though actually, like 15-20 years ago before AV engines were practically rootkits themselves, a broken/malfunctioning AV was a recognized sign of a virus/malware infection.

One that works? No. Thought that HVNC was for remote browser interaction. But fine, you have no way to create exclusions except physical access or gaining undetected remote access, bypassing UAC and any AV/EDR authentication, then creating exclusions to keep the FUD persistence mechanism from any future detection. Did I mention that a C:\ exclusion will immediately trigger an alert from Security Center?

Sure, that's a legitimate technique. Though if you haven't acquired the password and/or the system is behind a firewall and/or RD is unavailable, dropping AnyDesk can work, though it decreases stealth. And rootkits are rootkits. They can work. Sometimes they're rendered useless by patches.

d3athgiver - May 3, 2026, 5:15 pm

(May 3, 2026 02:11 PM)aerohacker Wrote: [\[CITE\]](#) And here we go again...

And you with these "intelligent", stupid sarcams and superficial answers... from someone who doesn't see beyond and doesn't think outside the box!

1 - That's exactly why uninstall any security solution would be ideal, whether it's AV/EDR... but even

the most lay user may notice that something is missing or at one time or another he or another more experienced user needs or wants to open or run an AntiVirus scan, so adding C:\ to the exceptions, would be a less suspicious option.

2 - Have you ever used HVNC or HRDP?!

3 - Another options would be install a legitim Remote Desktop tool, just in case the server would be detected and have a way to come back or Kernel Rootkit or Bootkit, that works on same AntiVirus level or start before Operating System, to keep FUD and the server persistent.

Understand one thing, when I ask questions, it's not just to clear up doubts, because as you yourself saw, I know what to do, but it's important to keep an open mind, read, see and think about other alternatives, this is called feedback.

When someone asks things like "which Operating System, AntiVirus, RAT, Crypter or another software is better?!" or which one do you use and why?!

It is not always a matter of doubt, but wanting to know the reason, pros and cons, and deeper answers of why someone prefers to use this than that.

A rat used some similar trick to run a gotohttp install and remote the victim. Make a binded version with a startup app and you can have acces for long time and it work pc amdroid isp pie linux and you remote device via browser

And for ceypthing it can crypt native payload but not support a specific rat, public stub get detected faster than private but you can make more ceypthed payload. You can get avr killer so you don't really NEED crypting but it's recommanded, you can also use silent exploit to infect device easily since people won't thrust a exe But bind a silent exploit to a app used at startup and you don't let suspicious track in the folders.

A script to run a reverse shell with shortcut high jacking to make it auto startup without showing any startuup app is the easiest way to do that. Remotely install a remote control app or get tue file you want and run command you want. Hrdp is worst garbage, when you start your pc you see another user account, you can make the device lag and bust yourself but using reverse shell to install something like hidden gotohttp you can control the device when it's inactive. There is also rat using pyzw exploit to drop drop terminal control on windows, don't need obfuscation or crypt but if you do this it bypass most av easily but require user to have python installed. Drop a python remote control script then you have full access

Voidlight - May 4, 2026, 7:52 pm

(May 3, 2026 10:20 AM)DramaKing Wrote: [\[CITE\]](#) So you're back with another highly intelligent post.

Excluding top-level directories is not always enough.

You have virtually no way to create exclusions without physical access.

You have as much chance of doing this as #2.

you can create exclusions via a uac bypass and powershell on most recent windows 11.

DramaKing - May 5, 2026, 2:01 am

(May 4, 2026 07:52 PM)Voidlight Wrote: [\[CITE\]](#) you can create exclusions via a uac bypass and powershell on most recent windows 11.

Voidlight, as much as I respect you, no. Running Set-MpPreference or changing registry keys with SYSTEM privileges are not enough to override the kernel driver. Maybe it's different where you are. I can provide a screenshot later.

possessed-client - May 5, 2026, 6:41 am

Doesn't replacing WD with another AV or using defendnot and then setting an exclusion work even with tamper protection on? Last time I checked it worked. Also, iirc there is publically available code for BYOVD tricks that allow to kill a lot of protected processes of AVs.

He B TeMy - May 5, 2026, 8:33 am

Guys, this discussion almost belongs in 2010/2014.

The truth is, remotely, without an exploit, you cannot bypass CURRENT Windows 11 protection that came in force early THIS year.

This includes the PUA protection, which is SEPARATE from DEFENDER and cannot be disabled via registry nor powershell (again, without exploit, which i don't know any).

It will block any "untrusted" applications from running, it does not matter if they're FUD or not, if you don't have a certificate, and a pretty good valid one, AND it's a "brand" new .exe, it will be blocked.

This puts a stick in the sand to most malware, you need physical access to turn this off.

As for AV exclusions, you can still do that with admin permissions ofcourse, but you need to disable Tamper Protection for IT to STICK (it will be applied, but Tamper will revert it, either on next reboot or next update)

So... without being superficial, read about it online about PUA, read about PowerShell Set-MpPreference like DramaKing said, and test it out yourself in a BRAND NEW VM running Windows 11.

on Windows 10 most of these will still work, but i'm talking Windows 11 here.

You speak about HVNC like it's magic stuff or whatever.

My suggestion to you is.... THINK, and start from the basics if you're old enough to have experienced anything before w10, and try to think what's the principle of it, and what ACTUALLY you want to do or not do.

There's plenty of ways still to achieve your goals, but it's getting increasingly harder day by day.

I'm not taking a shot a DramaKing, respectfully, maybe he could give you a little more advice, but the way you're writting, it's back from 2010 days with DarkComet running around.

Those "good" days will never come back. (good in quotes depending on your perspective)

Key information from this is, adapt, and test yourself on a brand new VM, fully updated, specially with April Service pack which brought and forcefully activated PUA on computers, ask me how i know.

possessed-client - May 5, 2026, 9:39 am

(May 5, 2026 08:33 AM)He B TeMy Wrote: [\[CITE\]](#) Guys, this discussion almost belongs in

2010/2014.

The truth is, remotely, without an exploit, you cannot bypass CURRENT Windows 11 protection that came in force early THIS year.

This includes the PUA protection, which is SEPARATE from DEFENDER and cannot be disabled via registry nor powershell (again, without exploit, which i don't know any).

It will block any "untrusted" applications from running, it does not matter if they're FUD or not, if you don't have a certificate, and a pretty good valid one, AND it's a "brand" new .exe, it will be blocked.

This puts a stick in the sand to most malware, you need physical access to turn this off.

As for AV exclusions, you can still do that with admin permissions ofcourse, but you need to disable Tamper Protection for IT to STICK (it will be applied, but Tamper will revert it, either on next reboot or next update)

So... without being superficial, read about it online about PUA, read about PowerShell Set-MpPreference like DramaKing said, and test it out yourself in a BRAND NEW VM running Windows 11.

on Windows 10 most of these will still work, but i'm talking Windows 11 here.

You speak about HVNC like it's magic stuff or whatever.

My suggestion to you is.... THINK, and start from the basics if you're old enough to have experienced anything before w10, and try to think what's the principle of it, and what ACTUALLY you want to do or not do.

There's plenty of ways still to achieve your goals, but it's getting increasingly harder day by day.

I'm not taking a shot a DramaKing, respectfully, maybe he could give you a little more advice, but the way you're writting, it's back from 2010 days with DarkComet running around.

Those "good" days will never come back. (good in quotes depending on your perspective)

Key information from this is, adapt, and test yourself on a brand new VM, fully updated, specially with April Service pack which brought and forcefully activated PUA on computers, ask me how i know.

What can I say, have to target people who are likely to be annoyed by PUA and have it off or would turn it off intermittently.

jason123 - May 5, 2026, 8:39 pm

(May 5, 2026 08:33 AM)He B TeMy Wrote: [\[CITE\]](#) Guys, this discussion almost belongs in 2010/2014.

The truth is, remotely, without an exploit, you cannot bypass CURRENT Windows 11 protection that came in force early THIS year.

This includes the PUA protection, which is SEPARATE from DEFENDER and cannot be disabled via registry nor powershell (again, without exploit, which i don't know any).

It will block any "untrusted" applications from running, it does not matter if they're FUD or not, if you don't have a certificate, and a pretty good valid one, AND it's a "brand" new .exe, it will be blocked.

This puts a stick in the sand to most malware, you need physical access to turn this off.

As for AV exclusions, you can still do that with admin permissions ofcourse, but you need to disable Tamper Protection for IT to STICK (it will be applied, but Tamper will revert it, either on next reboot or next update)

So... without being superficial, read about it online about PUA, read about PowerShell Set-MpPreference like DramaKing said, and test it out yourself in a BRAND NEW VM running Windows 11.

on Windows 10 most of these will still work, but i'm talking Windows 11 here.

You speak about HVNC like it's magic stuff or whatever.

My suggestion to you is.... THINK, and start from the basics if you're old enough to have experienced anything before w10, and try to think what's the principle of it, and what ACTUALLY you want to do or not do.

There's plenty of ways still to achieve your goals, but it's getting increasingly harder day by day.

I'm not taking a shot a DramaKing, respectfully, maybe he could give you a little more advice, but the way you're writting, it's back from 2010 days with DarkComet running around.

Those "good" days will never come back. (good in quotes depending on your perspective)

Key information from this is, adapt, and test yourself on a brand new VM, fully updated, specially with April Service pack which brought and forcefully activated PUA on computers, ask me how i know.

You are right ... I have tested something like that on two different Windows 10, The old windows without updates allowed WD to sleeping like dead while the second PC says nay! So basically those with older PCs are vulnerable while the New Windows need you to physical disable Tamper protection... The New Windows dislike this PowerShell Set-MpPreference but if any one has some tricks let us know...

Voidlight - May 6, 2026, 5:25 pm

(May 5, 2026 02:01 AM)DramaKing Wrote: [\[CITE\]](#) Voidlight, as much as I respect you, no. Running Set-MpPreference or changing registry keys with SYSTEM privileges are not enough to override the kernel driver. Maybe it's different where you are. I can provide a screenshot later.
I have working poc on latest build of win 11 not sure why it doesnt work for you

[Video: <https://vimeo.com/1189948898?share=copy&fl=sv&fe=ci>]

Edit for anyone curious, this uac bypass + ghostly hollowing combo that allows you to uac bypass a payload without dropping it to disk:

- Abuse appinfo RPC DebugObject hijack to leak a PROCESS_ALL_ACCESS handle from an auto elevated fodhelper session.
- Stage the payload in a delete pending state, capture the section handle, and trigger instant NTFS wipe while the code remains in memory.
- Spawn RegAsm.exe suspended with PROC_THREAD_ATTRIBUTE_PARENT_PROCESS spoofing to break process tree heuristics.
- NtUnmapViewOfSection the legitimate image and map the ghosted payload section into the elevated container.
- Hijack thread context and resume into the hollowed process.
- Payload resolves imports via manual PEB walking.
- Execute obfuscated PowerShell to add C:\ to defender exclusions

Pyr00 - May 6, 2026, 7:33 pm

(May 6, 2026 05:25 PM)Voidlight Wrote: [\[CITE\]](#) snip

Somewhat surprising defender doesn't detect this. Are you using syscalls?

I suspect most modern AVs would or definitely should detect this as they scan through memory so unmapping it isn't the hack it used to be. Obviously defender hasn't caught up.

Cool POC though.

DramaKing - May 7, 2026, 7:51 pm

(May 5, 2026 08:39 PM)jason123 Wrote: [\[CITE\]](#) You are right ... I have tested something like that on two different Windows 10, The old windows without updates allowed WD to sleeping like dead while the second PC says nay! So basically those with older PCs are vulnerable while the New Windows need you to physical disable Tamper protection... The New Windows dislike this PowerShell Set-MpPreference but if any one has some tricks let us know...

Exactly. Thanks for echoing my point.

(May 6, 2026 05:25 PM)Voidlight Wrote: [\[CITE\]](#) I have working poc on latest build of win 11 not sure why it doesnt work for you

[Video: <https://vimeo.com/1189948898?share=copy&fl=sv&fe=ci>]

Edit for anyone curious, this uac bypass + ghostly hollowing combo that allows you to uac bypass a payload without dropping it to disk:

- Abuse appinfo RPC DebugObject hijack to leak a PROCESS_ALL_ACCESS handle from an auto elevated fodhelper session.
 - Stage the payload in a delete pending state, capture the section handle, and trigger instant NTFS wipe while the code remains in memory.
 - Spawn RegAsm.exe suspended with PROC_THREAD_ATTRIBUTE_PARENT_PROCESS spoofing to break process tree heuristics.
 - NtUnmapViewOfSection the legitimate image and map the ghosted payload section into the elevated container.
 - Hijack thread context and resume into the hollowed process.
 - Payload resolves imports via manual PEB walking.
 - Execute obfuscated PowerShell to add C:\ to defender exclusions
- I don't care if you run obfuscated PowerShell as SYSTEM. Did you make sure that Tamper Protection was enabled? The driver will block any changes that aren't from Virus & threat protection.

Voidlight - May 8, 2026, 7:40 pm

(May 7, 2026 07:51 PM)DramaKing Wrote: [\[CITE\]](#) Exactly. Thanks for echoing my point.

I don't care if you run obfuscated PowerShell as SYSTEM. Did you make sure that Tamper Protection was enabled? The driver will block any changes that aren't from Virus & threat protection. if you watch the video you will see tamper protection is enabled.

Josh - May 8, 2026, 9:30 pm

(May 3, 2026 09:27 AM)aerohacker Wrote: [\[CITE\]](#) Once you've gained access to a PC and ensured persistence, what do you usually do to maintain persistence for as long as possible?!

- Add C:\ to the AntiVirus exclusions is enough or some module can one time or another detect the RAT server?!
- Uninstall the AntiVirus would be ideal, but this could generate suspicion.

had to check if the post was made in 2006 or 2026

simple answer is no, if that was as simple as that in this AI era, every kid in HF would be wiping his ass with 3 layers of \$100 bills.

MrAzalea - May 9, 2026, 2:48 am

(May 7, 2026 07:51 PM)DramaKing Wrote: [\[CITE\]](#) Exactly. Thanks for echoing my point.

I don't care if you run obfuscated PowerShell as SYSTEM. Did you make sure that Tamper Protection was enabled? The driver will block any changes that aren't from Virus & threat protection. There are definitely many ways to bypass Tamper Protection. Here is one example from me where it's clearly enabled and working, but an exclusion gets added anyway. Tested on latest Windows 11. [Video: <https://vimeo.com/1190708034?fl=pl&fe=sh>]

possessed-client - May 9, 2026, 12:31 pm

(May 6, 2026 05:25 PM)Voidlight Wrote: [\[CITE\]](#) I have working poc on latest build of win 11 not sure why it doesnt work for you

[Video: <https://vimeo.com/1189948898?share=copy&fl=sv&fe=ci>]

Edit for anyone curious, this uac bypass + ghostly hollowing combo that allows you to uac bypass a payload without dropping it to disk:

- Abuse appinfo RPC DebugObject hijack to leak a PROCESS_ALL_ACCESS handle from an auto elevated fodhelper session.
- Stage the payload in a delete pending state, capture the section handle, and trigger instant NTFS wipe while the code remains in memory.
- Spawn RegAsm.exe suspended with PROC_THREAD_ATTRIBUTE_PARENT_PROCESS spoofing to break process tree heuristics.
- NtUnmapViewOfSection the legitimate image and map the ghosted payload section into the elevated container.
- Hijack thread context and resume into the hollowed process.
- Payload resolves imports via manual PEB walking.
- Execute obfuscated PowerShell to add C:\ to defender exclusions

Nice writeup, but does the exclusion work and persist through reboots? I think there was a way to get an exclusion in the WD UI visually, while not actually having it function. Though there are ways to actually get it past Tamper Protection too, if yours is fully working, then looks like a very good and fast implementation.

Voidlight - May 10, 2026, 5:03 am

(May 9, 2026 12:31 PM)possessed-client Wrote: [\[CITE\]](#) Nice writeup, but does the exclusion work and persist through reboots? I think there was a way to get an exclusion in the WD UI visually, while not actually having it function. Though there are ways to actually get it past Tamper Protection too, if yours is fully working, then looks like a very good and fast implementation.

it is fully working on reboot and i know the method you're talking about where its just visual this is not that its a real exclusion. Thanks bro glad you thought it was cool.

possessed-client - May 11, 2026, 12:09 pm

Okay, I tried adding exclusions with powershell on a Windows 11 Pro 25H2 VM, and it worked when UAC elevated. So seems all you need is elevation after all, any UAC bypass would work. Talked to a LLM a bit, turns out Tamper Protection specifically does not cover exclusions. Not unless four conditions are met:

- 1.PC is managed by Microsoft Intune or Configuration Manager.

- 2.PC is onboarded to Microsoft Defender for Endpoint (MDE).
- 3.Defender for Endpoint Sense is enabled.
- 4.The DisableLocalAdminMerge policy is set to True (default value is Not Configured).

So unless a PC is included in some enterprise with a specific policy set to True by an administrator, Tamper Protection does not cover exclusions on the average consumer's PC, it only covers other settings.

A way to check whether Tamper Protection covers exclusions is this readonly registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features\TPExclusions . If 0, it does not cover, which seems to be default, from what I gather.

I don't know why I ever thought that Tamper Protection covers exclusions by default on all recent Win10/11, must be some sort of urban myth :D

DramaKing - May 14, 2026, 8:16 am

(May 11, 2026 12:09 PM)possessed-client Wrote: [\[CITE\]](#) Okay, I tried adding exclusions with powershell on a Windows 11 Pro 25H2 VM, and it worked when UAC elevated. So seems all you need is elevation after all, any UAC bypass would work. Talked to a LLM a bit, turns out Tamper Protection specifically does not cover exclusions. Not unless four conditions are met:

- 1.PC is managed by Microsoft Intune or Configuration Manager.
- 2.PC is onboarded to Microsoft Defender for Endpoint (MDE).
- 3.Defender for Endpoint Sense is enabled.
- 4.The DisableLocalAdminMerge policy is set to True (default value is Not Configured).

So unless a PC is included in some enterprise with a specific policy set to True by an administrator, Tamper Protection does not cover exclusions on the average consumer's PC, it only covers other settings.

A way to check whether Tamper Protection covers exclusions is this readonly registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features\TPExclusions . If 0, it does not cover, which seems to be default, from what I gather.

I don't know why I ever thought that Tamper Protection covers exclusions by default on all recent Win10/11, must be some sort of urban myth :D

I guess I made assumptions myself and have to eat crow. Can confirm by looking at Microsoft's blog. My elaborate Tamper Protection disable method no longer seems needed.

<https://techcommunity.microsoft.com/blog/microsoftdefenderatpblog/introducing-tamper-protection-for-exclusions/3713761>