

Forum: [Hack Forums](#)

Thread: [How to Bypass Antivirus with Simple Trick](#)

DramaKing - March 12, 2025, 3:59 pm

I was just hit with some inspiration and found this article:

<https://www.zdnet.com/article/snatch-ransomware-reboots-pcs-in-windows-safe-mode-to-bypass-antivirus-apps/> I don't know what registry key is used, but this specific method requires admin, anyway. If you have admin privs, you can likely disable AV or set exclusions without any hacks.

If you are not an administrator on your computer and want to disable AV, you should still be able to reboot to safe mode. You can either reboot to Advanced Startup from Settings or shift-clicking on the power button and restarting and choose Startup Settings or choose the Safe Mode restart option in msconfig.

When loading in Safe Mode, Windows only loads a minimum set of drivers. Antivirus drivers should not get loaded, meaning that the AV process either does not start or is unprotected. You should be able to run whatever you want now.

Do note that BitLocker and any TPM will ruin your cool hackz if enabled, and you don't have a key.

Binance - March 12, 2025, 4:04 pm

You're talking those with physical access?
People still do that?

DramaKing - March 12, 2025, 4:12 pm

(Mar 12, 2025 04:04 PM)Binance Wrote: [\[CITE\]](#) You're talking those with physical access?
People still do that?

They don't? And the Snatch ransomware group was working remotely, so one could find that registry key and code a Windows service. This partly goes back to [Centsicles](#)'s thread last year where he (supposedly) was on a limited user account and couldn't run any UAC bypasses or password recovery tools.

KrishnaGanga - May 2, 2025, 1:30 am

Solid breakdown! This Safe Mode AV bypass trick is a smart (though malicious) abuse of how Windows prioritizes minimal driver loading during boot.

As for the registry key, most malware including Snatch which modifies:

Code HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot
...to load its payload as a "critical" Safe Mode service. Some variants also set:

Code HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
to chain execution post reboot.

You're absolutely right though admin privileges are still the real gatekeeper here. If a threat actor has that, it's often game over regardless of clever tricks..

Also agree 100% on BitLocker + TPM. Once those are in place (and properly configured), Safe Mode or no you're not getting far without the keys.....

