

Forum:[Hack Forums](#)

Thread: [in need of help making .exe file bypass win defender](#)

kbizz420 - June 5, 2026, 11:52 am

hello, i am a beginner looking for some help, i have a .exe file that is embeded with xmrig, how can i get the .exe file to bypass windows defender because if it gets run then defender blocks it instantly. i have tested it in my VM on windows 10 but it just gets flagged by defender,

DramaKing - June 5, 2026, 12:22 pm

(Jun 5, 2026 11:52 AM)kbizz420 Wrote: [\[CITE\]](#) hello, i am a beginner looking for some help, i have a .exe file that is embeded with xmrig, how can i get the .exe file to bypass windows defender because if it gets run then defender blocks it instantly. i have tested it in my VM on windows 10 but it just gets flagged by defender,
Huh, thought WD didn't flag straight XMRig.

kbizz420 - June 5, 2026, 12:33 pm

(Jun 5, 2026 12:22 PM)DramaKing Wrote: [\[CITE\]](#) Huh, thought WD didn't flag straight XMRig.
yeah i dont really know, the rest of the system thats also binded with the .exe doesnt get flagged, its just the xmrig

MadScientist - June 5, 2026, 12:50 pm

(Jun 5, 2026 12:22 PM)DramaKing Wrote: [\[CITE\]](#) Huh, thought WD didn't flag straight XMRig.
Surprised it doesnt if so, so much malware drops it and WD even removed my damn official Monero Wallet

DramaKing - June 5, 2026, 1:45 pm

(Jun 5, 2026 12:33 PM)kbizz420 Wrote: [\[CITE\]](#) yeah i dont really know, the rest of the system thats also binded with the .exe doesnt get flagged, its just the xmrig
WD does not, in fact, flag the official signed XMRig binary even now, either because the signature makes it appear less malicious to heuristics or because Microsoft whitelisted it. You also mention that it's bonded. Binders themselves can have AV signatures. Or it's because there's no valid code signature. It's been shown that a self-compiled binary does get flagged.

<https://hackforums.net/showthread.php?tid=6323122&pid=62941158#pid62941158>