

Forum:[Hack Forums](#)

Thread: [\[Requires expert knowledge\] Do antivirus have capability of scanning running process?](#)

GhabXPH - March 31, 2014, 11:04 pm

Hello hack forums, I have something really concerned about. It is about the present level of security that anti-malwares implement to counter malicious softwares.

My question is: Does antiviruses/anti-malwares have capability of scanning running processes?

If that's the case, what would be the proposed countermeasures of known hacker papers to make their viruses hidden under such type of antiviruses?

If you're an expert or professional virus/malware author, what would be your proposition in dealing with such type of security?

And lastly, what particular antivirus do have such type of feature?

By discussing this topic, we may conclude the weaknesses of antiviruses/antimalwares, assuming a fact that they share the same methods of detecting algorithms, or perhaps, signatures. Otherwise if the result is negative, we may discuss further ways other than the suggested idea, to prevent antiviruses of detecting our coded malware. That's all guys :)

Disclaimer: The reason of this post is to test the several validities of theories in my mind. Thus, suggesting that I am just assuming and claim nothing. Just came here to clarify something and obviously, to learn. ?

id3vil - April 1, 2014, 1:34 am

varies for certain programs what antivirus software(s) are you using?

grady - April 1, 2014, 5:23 am

I'm no expert, but I know that they can scan running processes.

D4rKn3s5 - April 1, 2014, 6:34 am

Yes they scan running processes, and to my knowledge of them do. I believe they call it runtime protection, I could be wrong though. All you need to bypass it is get a RUNTIME FUD crypter, and it will still FUD to the AV when it's ran. As far as building it goes again, you'll just have to build it to be RUNTIME FUD.