

Forum:[Hack Forums](#)

Thread: [help in api hooking](#)

alexa872 - January 27, 2021, 1:43 am

so i am building a malware and i am having problems in hooking createProcess // openProcess , the main goal is to hook the run time check scan of windows defender (if anyone has better ideas let me know), bypassing the run time check is the hardest shit in av, specially if it is like machine learning AI and stuff like that.

what i need is help, sc maybe, hooking library, i dont want to go for the well known libraries because windows already patched them all and they are all not wrking now, much respect and i appreciate your time, thank you

FlowerontheMoon - January 27, 2021, 10:12 am

Are you building a web-based bot? If so let's talk! Did you already bypass the process memory? I just want to help for education purpose of course hahaha :)

alexa872 - January 27, 2021, 8:32 pm

(Jan 27, 2021 11:12 AM)FlowerontheMoon Wrote: [\[CITE\]](#) Are you building a web-based bot? If so let's talk! Did you already bypass the process memory? I just want to help for education purpose of course hahaha :)

it is not web based bot, i am targeting windows 10, i had a trojan that worked for a while and now it is getting detected as sunburst !!!!!!! idk wtf but wtf, i want these hooks to bypass the dynamic scan aka run time check and that is it. if you want to get into details, im in, and ill be more than happy to get some help and share experience with each other

notebook - January 29, 2021, 10:35 am

Try passing "CREATE_SUSPENDED" as a flag to suspend the process/thread, then injecting/passing whatever code, and then resume by calling "ResumeThread", Not sure if it would work but you could use this in a dropper and drop the actual bot then resume the process after it's dropped. Not sure if this would work in a real enviroment though

alexa872 - January 29, 2021, 8:41 pm

(Jan 29, 2021 11:35 AM)notebook Wrote: [\[CITE\]](#) Try passing "CREATE_SUSPENDED" as a flag to suspend the process/thread, then injecting/passing whatever code, and then resume by calling "ResumeThread", Not sure if it would work but you could use this in a dropper and drop the actual bot then resume the process after it's dropped. Not sure if this would work in a real enviroment though

so i was messing around for a solution and i found this =>

aHR0cHM6Ly9sYWJzLmYtc2VjdXJlLnNvbS9ibG9nL2J5cGFzc2luZy13aW5kb3dzLWRlZmVuZGVyLXJ1bnRpbWUtc2Nhbm5pbmcv

i liked the idea... so i went to where they posted there code on github, the problem that the code is not real 100% and contains a lot of code && header files missing

i went on github and searched for another hooking library and i found some, but the problem is that there is a big number of these libraries patched by security companies, and some of them contain dll files to perform the hook which is kinda useless, i will then need to upload 2 files to perform the trick, and the other libraries are just too big, it will effect the size of my program, i have been looking/trying for a while now, so i kind of given up, but from time to time i just want to mess around and some

post give me hope again and then i fk up (again), i got a really good idea to build, but it is just not working, the malware cycle i am thinking of is much more complicated than normal rats that will just decrypt and inject, i am building something may need months, but again its been a months, although i made some nice code till now, so idk man, you may think that i am one of these kidies around... message me so that ill explain more.

anyways i really thank you for your time and attention, and have a nice day !

duxv5600 - September 7, 2021, 12:28 pm

(Jan 29, 2021 09:41 PM)alexa872 Wrote: [CITE](#) so i was messing around for a solution and i found this =>

aHR0cHM6Ly9sYWJzLmYtc2VjdXJlLnNvbS9ibG9nL2J5cGFzc2luZy13aW5kb3dzLWRlZmVuZGVyLXJ1bnRpbWUtc2Nhbm5pbmcv

i liked the idea... so i went to where they posted there code on github, the problem that the code is not real 100% and contains a lot of code && header files missing

i went on github and searched for another hooking library and i found some, but the problem is that there is a big number of these libraries patched by security companies, and some of them contain dll files to perform the hook which is kinda useless, i will then need to upload 2 files to perform the trick, and the other libraries are just too big, it will effect the size of my program, i have been looking/trying for a while now, so i kind of given up, but from time to time i just want to mess around and some post give me hope again and then i fk up (again), i got a really good idea to build, but it is just not working, the malware cycle i am thinking of is much more complicated than normal rats that will just decrypt and inject, i am building something may need months, but again its been a months, although i made some nice code till now, so idk man, you may think that i am one of these kidies around... message me so that ill explain more.

anyways i really thank you for your time and attention, and have a nice day !

aHR0cHM6Ly9sYWJzLmYtc2VjdXJlLnNvbS9ibG9nL2J5cGFzc2luZy13aW5kb3dzLWRlZmVuZGVyLXJ1bnRpbWUtc2Nhbm5pbmcv

->

<https://labs.f-secure.com/blog/bypassing-windows-defender-runtime-scanning/>

i hope i helped you