Windows Anti-Debugging & Anti-ANti-Debugging Techniques

Arash TC

Windows
Anti-Debugging
&
Anti-Anti-Debugging
Techniques

Contents

Why?

As I got obsessed with documenting everything I learn in a way that if I lose my memory, I can learn them again from the ground up, I decided to prepare a write up on Anti-Debugging and Anti-Anti-Debugging Techniques performed on Windows operating system. This paper will not include pseudo code like lots of other blogs or paper you see (or at least I see.) but it will provide proof of concept code in C++ with hands-on examples. This paper will eventually turn into a book as I add new content because these techniques will never end and depending on your knowledge base and creativity, you can invent your own.

About the Author

It's me again, Arash TC, (the low level security dude :D). One thing you definitely agree on about me (hope so) is that I don't spam the reader with unnecessary bullshit telling people about the history of assembly language or how my high school friend wrote a kickass virus with library's computer. You open the book, you jump into the actual content. Free of charge as usual because who am I to charge people for gaining knowledge. Remember to Learn and Contribute.

What about Linux?

The Linux part will be handled by my friend Kami[1] and the content will be uploaded (or maybe is uploaded by the time you're reading this) in the same github repository.[2]

Can I use the content in other ways?

Yes. Whatever creative commons lets you to. Specific license file is in the repository.[3]

---

[1] https://twitter.com/_k4m1_
[2] https://github.com/Captainarash/Reverse-Engineer/tree/master/Anti-Debugging%20and%20Anti-Anti-Debugging/Linux
[3] https://github.com/Captainarash/Reverse-Engineer/blob/master/LICENSE