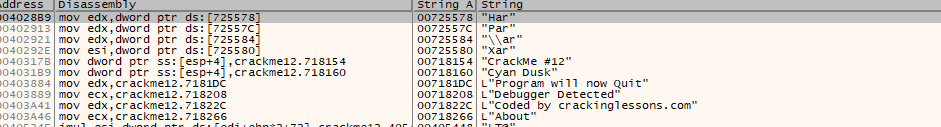


This crackme is all about anti-debug technique

Object is bypass all anti-debug feature

Throw into x32

Find references string



We found a “Debugger Detected” and “Program will now Quit”

Let’s jump there!

We see that, crackme calls a function IsDebuggerPresent, and the result is compared with 0.

If it is not 0, the bad block contain “Debugger Detected” will be executed.

Read the MSDN of this API, we found that if the result of this function returns not 0, which means the program is run under a debugger. So to bypass this, we can patch je into jne

