Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sat, 02 Jun 2018 10:34:20 GMT
View Forum Message <> Reply to Message

By now I'm testing first code on GCC, 64 bit, both in debug and release mode and it works perfectly.
The only caveat is that I can't set a different encrypting NONCE for each function as before, because there's no
simple way to embed data into the code as I coud do in assembly.
Not a big concern, just a bit less secure and probably crackable if you have a ton of encrypted functions, but
strong enough for most purposes.
I'm fixing the obfuscation part, then I'll go to windows.
It has NO inline assembly code inside, and there are just 2 conditions:

- encrypted code should contain NO data (which AFAIK is always true)
- the compiler should not re-arrange the code so that marked end comes before marked start. This should also be
always true but, if not, the encryptor will notice and signal it.

Code is encrypted only on its first byte of each instruction; remainig bytes and data fields are left unchanged.
This is more than enough to make the program crash if incorrectly decrypted, and avoids fiddling with fields changed
by loader (as far addresses, for example).
It should work on any X86 / X86-64 compiler with minor changes.