Subject: Re: Moving on with supporting old things...
Posted by mdelfede on Thu, 18 Feb 2016 14:56:04 GMT
View Forum Message <> Reply to Message

Hi,

sorry for my lack of time to fix protect.... we'd need indeed some other way to implement it, in particular because of
lacking of inline assembler in 64 bit code.
The "scramble just the opcode" way would be a nice workaround, but only for 32 bit windows.

I think that it would be possible to implement a pure C solution, with help of a couple of external assembly routines, but it needs much work and some time which I don't have right now.
I'm just dropping here my idea: we could put a call in front of to-protect code :

.....
DecodeMe(0xaa, 0x23, 0x55, 0x44.....some-unique-byte-pattern);
.... some code to encrypt
DecodeEnd(0xaa, 0x23, 0x55, 0x44.....some-unique-byte-pattern);

DecodeMe function should be written in pure assembly, and should use return address to locate the code to change.
The DecodeEnd should be a dummy function in order to have an "end pattern" to know where code ends.
In assembly such calls should contain be a sequence of PUSH number PUSH number....., so quite easy to locate, both from external encoder and to internal decoder code.

DecodeMe() function should of course decode just the op-codes as Mirek suggestion.
If I'll find some spare time I'll try to implement it.

Ciao

Massimo