Subject: Re: Protect packages - split code encryption,client and server
Posted by mdelfede on Wed, 07 Aug 2013 21:18:18 GMT
View Forum Message <> Reply to Message

So, we can try this, but it mus be done on your friend's machine.

1) Remove PROTECT_START_FUNC and END_FUNC macros from your protected function and replace them with the code in Protect.h (remove the backslashes, of course), so you can step inside macros with debugger.

2) Build the app, but do NOT run the ProtectEncrypt on it. Step up to protected function beginning, note the code range of the function, dump it on a file. Name it as UNENCRYPTED.BIN. The difficult part is to find the end of he cunction inside binary code, but you can search for PROTECT_END_MARKER byte sequence.

3) Run ProtectEncrypt on app, then do the same as before. Beware to stop BEFORE the call to Decrypt function.
Store the code area inside ENCRYPTED.BIN file. Take care it has the SAME length as former one.

4) Without exiting debugger, step OVER the decrypt function call, and re-save the binary code inside DECRYPTED.BIN file.
As before, the file should have same length as 2 former files.

5) You can send me the 3 binary files, if you trust. Otherwise, compare the UNENCRYPTED.BIN file with the DECRYPTED.BIN file. They should be identical, besides the marker (PROTECT_START_MARKER and PROTECT_END_MARKER which gets overwritten by ProtectEncrypt.
If there are other differences besides markers, try to locate them.... if they're near end marker, the decrypt routine is missing some parts.

You could also check if ProtectEncrypt do its job on the whole code between both markers, by comparing UNENCRYPTED and ENCRYPDET files. That could give some hints too.