Subject: Re: Considering different approach to Win32 release
Posted by mirek on Mon, 02 Nov 2015 16:17:51 GMT
View Forum Message <> Reply to Message

OK, so I have digged deep into the protect and found the problem...

...well, the problem is that it cannot work the way it is designed...

```
double CryptedTest(double d, double e)
{
 PROTECT_START_FUNC(Decrypt);

 double f;
 f = d * e;

 PromptOK("CryptedTest DECRYPTED SUCCESFULLY!!!");
 return 2 * f + e;

 PROTECT_END_FUNC;
}
```

The problem here is that ProtectEncrypt absolutely ignores any linker fixups. This means that literal string constant in PromptOK gets encrypted 'raw'. Then, when program is run, .exe loader relocates *encrypted data*, and they get decrypted only after relocation, resulting in wrong address (that is why it crashes) and possibly broken decryption.

So, for now, if you need to use Protect, the only code it might be able to handle is the one that does not reference static data or other functions.