Subject: Protect package - A starting copy protection system
Posted by mdelfede on Sun, 19 Sep 2010 19:07:57 GMT
View Forum Message <> Reply to Message

I added a symple code copy protection / encryption package (Protect) with the encryptor itself (ProtectEncrypt) and a test application (ProtectTest).

Please read the help inside Protect package in order to setup the encryptor.
Once properly setup, the system is transparent to TheIde build system; code will be automatically encrypted upon build.

Please try it with the ProtectTest demo package:

1) Load and build ProtectEncrypt package; if possible put the resulting executable somewhere in your execution path (/usr/bin for Linux, system32 directory for windows). If you prefere, you can leave executable in upp/out folder, but you'll have to give the full executable path to custom build step, see below.

2) Open the demo project ProtectTest; choose the 'GUI PROTECT' build flags AND update the custom build step to match location of your ProtectEncrypt executable; please leave the demo KEY as it is.

3) Build and run the ProtectTest package. If all went OK, you'll see a couple of message boxes telling you that, OR possibly you didn't choose the 'GUI PROTECT' build flags, in which case the encryptor isn't operating.

4) When all above is working, try to change the key inside GetKey() function in ProtectTest package, making it different from the one inside the custom build step line.
Running the app will make it crash, as it'll be executing garbage code instead of un-encrypted one.

REMARKS :

-- if you don't choose the 'GUI PROTECT' build method, encryption will be disabled and your app will run unprotected.

-- if you don't put the right executable path on custom build step, the encryptor won't work, BUT the decryptor inside test app will... so you'r app will crash when run.

This one IS NOT a commercial grade copy protection system, but just a starting point for software locking/encryption; feel free to add suggestions/enhancements to it !

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by dolik.rce on Sun, 19 Sep 2010 22:50:38 GMT
View Forum Message <> Reply to Message

Hi Max!

This is a very interesting package. I couldn't resist and played with it for a while My conclusions: It works very well and it would definitely stop me from stealing the app.

Few observations:

It works as well with flags "GUI .PROTECT" which cause less recompilation when switching between protected and unprotected mode. (If you want to have encrypted code in other packages than main and still use this trick, you can add PROTECT into 'Accepts' field in package manager.)

You can't declare variables inside the encrypted block, because 'jump to label __end crosses initialization of ...'. It is somewhat cryptic, so it should be probably mentioned in docs. Work around is to put another pair of '{}' between the calls to PROTECT_... macros to limit the scope of variables declared inside.

You can't have two encrypted blocks in one function, as it results into redeclaring variables. Even if the blocks are in different scopes, it fails on duplicate labels. This could be fixed easily, but it is probably not important for real-life usage.

The 'return' in PROTECT_END_FUNC prevents using the macro in functions returning a value. Omitting it causes runtime error, but ugly fix comes to my mind:#define
//only for posix here, for win it is similar
```
PROTECT_END_FUNC(RETURN) \
 RETURN; \
 __end: \
 asm volatile ( \
  "\t.ascii \""PROTECT_END_MARKER"\"\n" \
 )
//and calling it like this (stupid example):
int testfn1(void){
 int j=0;
 PROTECT_START_FUNC(Decrypt);
 PromptOK("testfn1 DECRYPTED SUCCESSFULLY!!!");
 return j; // <- returning in between wouldn't hurt
 PROTECT_END_FUNC(return j);
}
```

One question at the end: Do I understand it right, that the decryption is performed only on first call of the function? So it modifies only the program loaded in memory? If so, I'll seriously consider calling it a voodoo

Good job!
Honza

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Mon, 20 Sep 2010 06:14:18 GMT
View Forum Message <> Reply to Message

Thank you Massimo

I will try to use it, sure!

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Mon, 20 Sep 2010 08:02:06 GMT
View Forum Message <> Reply to Message

dolik.rce wrote on Mon, 20 September 2010 00:50Hi Max!

This is a very interesting package. I couldn't resist and played with it for a while My conclusions: It works very well and it would definitely stop me from stealing the app.

Ehehehe.... no, it's not too difficult to defeat, IF you've the key

Quote:
Few observations:
.....
You can't declare variables inside the encrypted block, because 'jump to label __end crosses initialization of ...'. It is somewhat cryptic, so it should be probably mentioned in docs.

mhhhh... I haven't tried it enough, but I guess it can be solved
somehow.... I couldn't just resist to put on bazaar for testing
The main problem I found is that damned M$ inline assembler, I guess it was coded by some drunk people....

Quote:
Work around is to put another pair of '{}' between the calls to PROTECT_... macros to limit the scope of variables declared inside.

I'll look at this solution this night.... Maybe it's a good suggestion

Quote:
You can't have two encrypted blocks in one function, as it results into redeclaring variables. Even if the blocks are in different scopes, it fails on duplicate labels. This could be fixed easily, but it is probably not important for real-life usage.

Well, the macros are thought for single usage in every function. I guess they could be modified for multiple usages (maybe using the __LINE__ macro for labels, or something like that, but I guess it's better to use it just once per function.

Quote:
The 'return' in PROTECT_END_FUNC prevents using the macro in functions returning a value.

Omitting it causes runtime error,

Well, that's a bigger problem.... I didn't think about it.
The ending return statement is just to avoid entering into data (garbage) part of the code.... But can be solved also with an assembler jmp, I guess. I'll try it this night too

Quote:
One question at the end: Do I understand it right, that the decryption is performed only on first call of the function? So it modifies only the program loaded in memory? If so, I'll seriously consider calling it a voodoo

Yep, it's decrypting on the fly on first function call.... and that's the biggest flaw of the approach. With a good placed breakpoint you can have the decrypted code in memory, and looking for the call to decrypt routine is quite easy with a good debugger. You must, indeed, have the key handy to do that, without key you can't do anything.
I was thinking about obfuscating a bit more the stuff, I've just to think a bit about it. The "big" problem is to keep the process simple and portable between GCC and MSC; to do a better think we should parse executable headers which isn't easy.

Anyways, as you can see from macro code, the whole process isn't a big voodoo The macro just marks the executable with some known strings, easily found by encrypter code, which patch the executable on right places. The decrypter has just to open code memory for write access and reverse the process. It's easy if you use encrypt algorithm that doesn't change code size.
A better (and more secure) approach would be to encrypt/pack the code and to decrypt/unpack in memory allocated for the purpose.... But, I guess then ww would have do parse executables, object files and so on, which makes it a nightmare for portability sakes

Quote:
Good job!
Honza

Thank you

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Mon, 20 Sep 2010 11:57:02 GMT
View Forum Message <> Reply to Message

Uhmmmm... well, I guess the 2 most annoying points are solved now.

Now functions returning values are allowed and also declarations inside function body.

Ciao

Max

Edit: btw, if somebody just wonders why the

```
if(!__decrypted)
   goto __end;
```

Is needed (goto is never taken), that's because if not there the optimizing GCC would skip the end marker assembly code, thinking it never gets executed.

Subject: Re: Protect package - A starting copy protection system
Posted by dolik.rce on Mon, 20 Sep 2010 16:29:03 GMT
View Forum Message <> Reply to Message

Wonderful!

I have one more idea Unfortunately I am too lame to implement it

Just letting it crash by executing garbage is not really nice (even if the cheating user deserves it). Might be even possibly dangerous. Would it be possible to somehow check if the decryption was successful and throw an exception? Then the programmer could use something like

```
bool TestLicense(){
   bool b;
   try{
      PROTECT_START_FUNC(decrFunc);
      b=true;
      PROTECT_END_FUNC;
   }catch (...) {
      Exclamation("Invalid license, get a new one!");
      b=false;
   }
   return b;
}
```

Now implementation idea: put one more data section similar to PROTECT_XY_MARKERs, but this time into the encrypted area. As this would be a known constant, it could be checked right after decrypting. If the decrypted data don't match, the inner function code could be skipped and exception thrown (or some flag raised, if you don't like exceptions). Do you think this would be possible?

Honza

PS: Sorry if it looks like I am never satisfied I admire the code and just trying to give you a

(possibly useful) feedback

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Mon, 20 Sep 2010 19:38:15 GMT
View Forum Message <> Reply to Message

Well, the idea is to check the license correctness at program startup and abort if not valid.... You should never reach the encrypted functions if license is not valid.
The check could be quite simple, like that one :

```
main()
{
   String guard = "someencryptedtextofwhichyouknowthedecryptresult";
   String key = GetGey();
   Buffer<byte>buf(guard.GetCount());
   memcpy(buf, ~guard, guard.GetCount());
   RC4 rc4(key);
   rc4.Crypt(buf, buf, guard.GetCount());
   if(strncmp(buf, "yourknowndecryptedtext", guard.GetCount())
   {
      PromptOK("Invalid license key!!!");
      exit(1);
   }

   // here rest of your app

}
```

As you see, the user is warned that the key is invalid. If it
patches the app, for example removing the exit(), he deserves a good app crash

Purpose of encryption is to (try to) avoid reverse engineering of application, not to signal the user of the correctness of license.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by dolik.rce on Mon, 20 Sep 2010 21:21:14 GMT

mdelfede wrote on Mon, 20 September 2010 21:38As you see, the user is warned that the key is invalid. If it
patches the app, for example removing the exit(), he deserves a good app crash
Point taken I don't know why I always miss the simple solutions

Honza

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Mon, 20 Sep 2010 21:38:59 GMT

dolik.rce wrote on Mon, 20 September 2010 23:21mdelfede wrote on Mon, 20 September 2010 21:38As you see, the user is warned that the key is invalid. If it
patches the app, for example removing the exit(), he deserves a good app crash
Point taken I don't know why I always miss the simple solutions

Honza

Well, I think I'll add some simple encrypt routines for strings and a macro to check the correctness of key... they should be simple too.
Btw, I'd like to add a simple web authentication scheme... do you have some skill in php/web programming ?
What I'd need would be a way to register by app dialog, get back an activation e-mail with a link and then have the key sent from web server to my app on each app run.
I mean :

APP NOT REGISTERED --> REGISTER DIALOG --> SEND TO SERVER
SERVER SENDS EMAIL --> USER CLICK ON EMAIL LINK -- USER ACTIVATED

On following app launches :

APP REGISTERED --> ASK SERVER FOR KEY (sending name-mail-pass) --> SERVER SEND BACK KEY

The best would of course be some obfuscation of key from server, but that one could be added later.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Tue, 21 Sep 2010 22:52:53 GMT
View Forum Message <> Reply to Message

I added some more stuffs to package :

1) A macro to check key correctness on startup :

```
ON_PROTECT_BAD_KEY(Decrypt)
{
   PromptOK("Bad License !!!");
   exit(1);
}
```

And another protection method, OBFUSCATION, which is handy to make code hard to disassemble/debug even before you obtain the key, so useful to protect your key-obtaining code sections, for example.

Docs and example have also been updated.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Thu, 23 Sep 2010 15:05:55 GMT
View Forum Message <> Reply to Message

Does somebody have the sources (C, possibly....) of the snow 2.0 cypher algorhitm ? I've looked at their website and is gone... Also googling around didn't give me hints.
The RC4 used by now is quite weak.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Thu, 23 Sep 2010 18:39:34 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Thu, 23 September 2010 17:05Does somebody have the sources (C, possibly....) of the snow 2.0 cypher algorhitm ? I've looked at their website and is gone... Also

googling around didn't give me hints.
The RC4 used by now is quite weak.

Ciao

Max

Hello Massimo

In AESStream you have AES, that is rather safe.

It works very well.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 24 Sep 2010 08:13:40 GMT
View Forum Message <> Reply to Message

Hi Koldo,

I'll try it, maybe.
I would have liked a builtin solution, as I need to encrypt short pieces of code and I guess there is need to change somehow the key from one to another to keep it safe.
Having many small chunks encrypted with the same key (and same startpoint of key random generation) is the best way to have your key cracked

Thank you for the hint !

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Zbych on Sat, 25 Sep 2010 11:36:57 GMT
View Forum Message <> Reply to Message

AES is quite small. See attached files that implement AES256 encryption. I use them on small 8-bit uC like AVR.

File Attachments
1) aes256.zip, downloaded 416 times

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sat, 25 Sep 2010 13:37:13 GMT
View Forum Message <> Reply to Message

Zbych wrote on Sat, 25 September 2010 13:36AES is quite small. See attached files that implement AES256 encryption. I use them on small 8-bit uC like AVR.

Hi Zbych,

thank you for the source
As I see, AES is a block-encoder with a blocksize of 128 bits and a keysize of 128, 192 or 256 bits, right ?
If so, I'll have to adapt it to my routines, as they need to encode/decode variable sized buffers.
Just one question : if I encode 2 128 bit blocks, let's say block 1 and block 2, and I want to decode them in reverse order, like block 2 and then block 1, shall I care about something, like resetting the encoder between blocks ?

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Zbych on Sat, 25 Sep 2010 16:03:28 GMT
View Forum Message <> Reply to Message

Those routines implement ECB (electronic codebook) mode. That means that every block of data is encoded separately. It is safer to use CBC mode with long data streams.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

If you use ECB mode, you don't have to reset encoder, just initialize ctx at the begging. Since you want to encrypt blocks of code, you can tell compiler to align code to 16 bytes (in case of gcc you can add inline assembly with align directive).

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sat, 25 Sep 2010 16:59:10 GMT
View Forum Message <> Reply to Message

Ah, ok, I got it

Anyways, I need to cypher each code routine separately, as they are decyphered in random order (when they're used), so I guess I could do CBC restarting it on each encrypted routine... Or,

maybe, use CBC plus some random data added at beginning of each routine, which should lead to different coding even for identical routines.
The most annoying problem is the need of padding to 128 bits buffer, which makes it impossible to code directly on place.

Thank you for your hints

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 29 Sep 2010 20:29:18 GMT
View Forum Message <> Reply to Message

Well, I finally found Snow2 code, so I replaced the endoding method in Protect package from RC4 to Snow2.
This brings far more encryption security at the expense of a small increment of code footprint.
A small caveat : Snow2 requires a key of fixed length of 16 OR 32 bytes (128 or 256 bits); other keylengths are NOT supported.

The encryption code is removed from Protect package and added as a new (StreamCypher) package wich implements both RC4 and Snow2 encodings.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Thu, 30 Sep 2010 19:30:18 GMT
View Forum Message <> Reply to Message

Hi Max,

Great stuff. Can't wait to get the time to get to know it better.

BTW: Do you take suggestions? If you do, may I suggest adding detection of and protection against common cracking debuggers such as SoftICE and like? This kind of reverse engineering protection is commonly found on the commercial protection products such as former Aladdin HASP HL now Safenet Sentinel HASP HL and Matrix Software Protection.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Thu, 30 Sep 2010 20:59:01 GMT
View Forum Message <> Reply to Message

Eh. Tom... SoftICE detecting is quite windows-specific, and I develop on Unix only
I'd need some window system programmer to partecipate on the package.
BTW, I think that to make it a semi-professional copy protection package we should add much more hardening stuffs, which is quite difficult keeping it portable between both worlds (and maybe also to other platforms).

Anyways, dolik-rce and I we're preparing a web-authentication module to be used together with Protect, which will allow registering and auth through a web server, which, BTW, is a thing I need for my app

Next I could try to give a look to some dongle auth stuff, I'm good enough on electronics, so I could develop a dongle hardware well suited to Protect package, and I've got also an electronic manufacturer that can prototype it even in small quantities for few money
I've already some ideas on how to do it... Just no time by now !

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Fri, 01 Oct 2010 06:11:24 GMT
View Forum Message <> Reply to Message

Hello Massimo

All of this sounds very good.

Many people here are freelance or work in small companies without money to pay the very expensive commercial protections available.

Web-authentication sounds great and dongle is also interesting.

If you need windows specific things I can help.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 01 Oct 2010 11:53:45 GMT
View Forum Message <> Reply to Message

Hi Koldo, thanks for your help
By now dolik-rce is helping with PHP parts, I guess that's the easiest (and more portable way) to do it.
I'd like to have the encryption package ported there, as we need it to communicate with server in encrypted form... he's working on it.
About the windows part.... the missing stuffs are debugger detection AND some better hardening tools, but then I guess we'll have problems to keep all that compatible between words.
Also GDB detection wouldn't be bad, but I've no idea on how to do it.

Anyways, the most weak of my protection scheme is that the decoding parts are fixed and traceable.
It wouldn't be bad to make them variable and somehow autodecoding... but that can be done later.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by 281264 on Fri, 01 Oct 2010 19:53:19 GMT
View Forum Message <> Reply to Message

Massimo,

How can I download the package?

Cheers,

Javier

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 01 Oct 2010 20:36:56 GMT
View Forum Message <> Reply to Message

281264 wrote on Fri, 01 October 2010 21:53Massimo,

How can I download the package?

Cheers,

Javier

It's in Bazaar, just use svn or fetch latest nighty builds, it should be there.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by 281264 on Sat, 02 Oct 2010 14:00:57 GMT
View Forum Message <> Reply to Message

Hi Massimo,

I am finding some unexpected outcome. The problem seems to be related with the key. The encryption key I am using is AABBCCDDEEFF00112233445566778899 (as shown, without quotes); the GetKey function is as the example:

```
String GetKey(void)
{
 // WARNING -- TO PUT A NULL BYTE (0X00) INSIDE KEYSTRING
 // REQUIRES SOME ADDITIONAL WORK !
 String k = "\xAA\xBB\xCC\xDD\xEE\xFF";
 k.Cat('\x00');
 k += "\x11\x22\x33\x44\x55\x66\x77\x88\x99";
 return k;
}
```

The application compiles well and it runs fine, but it does not recognize the kye!

Where is the bug?

Remarks:

2.- what is len in the PROTECT_DECRIPT function? The length of the key, perhaps (the it should be 16bytes or 32 bytes)?

Thank you,

Javier

Subject: Re: Protect package - A starting copy protection system

281264 wrote on Sat, 02 October 2010 16:00Hi Massimo,

I am finding some unexpected outcome. The problem seems to be related with the key. The encryption key I am using is AABBCCDDEEFF00112233445566778899 (as shown, without quotes); the GetKey function is as the example:

```
String GetKey(void)
{
 // WARNING -- TO PUT A NULL BYTE (0X00) INSIDE KEYSTRING
 // REQUIRES SOME ADDITIONAL WORK !
 String k = "\xAA\xBB\xCC\xDD\xEE\xFF";
 k.Cat('\x00');
 k += "\x11\x22\x33\x44\x55\x66\x77\x88\x99";
 return k;
}
```

The application compiles well and it runs fine, but it does not recognize the kye!

Where is the bug?

The bug is that your encryption key is AABBCCDDEEFF00112233445566778899 but in your source you use AABBCCDDEEFF.... Keys in optional build step command line and inside your code must match.

Quote:
Remarks:

well, you can use whathever you like, it's enough that keys are 16 or 32 byte long.
Of course, for sake of simplicity, the key in custom build step is entered as hex-ascii string, so AABB.... where each couple of chars form an hex byte, otherwise it would be hard to enter keys with control chars there.
If you enter for example 303132333435 in custom build step, the key in your code should be any of :
[code]
12345
\x30\x31\x32\x33\x34\x35
[/quote]
I'd suggest the second form as it's easy to compare with the custom build step one.....

2.- what is len in the PROTECT_DECRIPT function? The length of the key, perhaps (the it should be 16bytes or 32 bytes)?
[/quote]

PROTECT_DECRYPT is an helper function which takes following parameters :

Address of the block to be decoded
Length of the block
A String containing the key

In your case you should use :

```
bool Decrypt(byte *start, size_t len)
{

    return PROTECT_DECRYPT ( start, len, GetKey());

}
```

Where the GetKey() function is your above one.

Anyways, I guess I've to change the help a bit.....

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sun, 03 Oct 2010 20:49:08 GMT
View Forum Message <> Reply to Message

Changed Protect to use new Cypher encryption package.
Added handling of IV (initialization vectors) on encryption to harden security.
Now 2 identical functions encrypts differently.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Fri, 08 Oct 2010 10:29:33 GMT
View Forum Message <> Reply to Message

Hello Massimo

What is the status of this?

Quote:Anyways, dolik-rce and I we're preparing a web-authentication module to be used together with Protect, which will allow registering and auth through a web server, which, BTW, is a thing I need for my app

---

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 08 Oct 2010 12:10:13 GMT
View Forum Message <> Reply to Message

Hi Koldo,

I'm quite busy on these days, but I'm developing an SCGI solution alternative to PHP one.
So, I'm working on SCGI and dolik-rce on PHP, we'd like to post both with a common interface.
I guess we'll need a couple of weeks or a bit more... not too much time on these days

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sun, 10 Oct 2010 12:35:32 GMT
View Forum Message <> Reply to Message

Protect Client/Server auth development is progressing.
In Bazaar you'll find following stuffs :

Protect package, with added ProtectServer and ProtectClient classes

ProtectServerDemo, a demo SCGI protection server
ProtectClientDemo, a demo SCGI protection client

It's all still in very early development phase, in particular database connections on server side is still missing (I've to learn how to do it)

Anyways, the encrypted connection works quite well, and client/server communication is quite reliable.

When more advanced I'll put the demo server on my remote server; by now, to test it you have to setup an HTTP server (I'm using Apache2 on ubuntu or on centos), add mod_scgi module, enable it and so on.... Not a difficult task but you must google for some docs.

I'll add some docs when finished.

Some technical details :

Client/Server communication is done via encrypted xml data, so it's not possible to gather application key sniffing web traffic.

Encryption is done by Cypher package, defaulting to Snow2 encryptor, but you can optionally switch to RC4 and other (future) encryptors added to Cypher package.

Client/Server Protocol is SCGI (thanx Jeremy!!)

Feel free to add suggestions to the package and/or to help with MySql database stuff !

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Tue, 12 Oct 2010 23:06:08 GMT
View Forum Message <> Reply to Message

I posted last version of web authentication package.
Still no docs, but code is enough self explaining.

As before, there's a ProtectServerDemo and a ProtectClientDemo test apps.
All work besides license activation, mail is sent but the activation link is still not ready.

To test it, as before, you shall setup an http server with SCGI module installed.... By now I'd suggest it only for people experienced enough.

On next days I'll setup the test server.

The app supports multiple licensing, timed demo, check for multiple runs of the application and so on.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Wed, 13 Oct 2010 07:11:02 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Fri, 08 October 2010 14:10Hi Koldo,

I'm quite busy on these days, but I'm developing an SCGI solution alternative to PHP one.

So, I'm working on SCGI and dolik-rce on PHP, we'd like to post both with a common interface.
I guess we'll need a couple of weeks or a bit more... not too much time on these days

Ciao

Max

Great!

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 13 Oct 2010 23:42:16 GMT
View Forum Message <> Reply to Message

Hi,

Now in bazaar there's a demo of my client/server app to get encryption key, along with a demo server installed on a remote machine.

To test, just run the client, register with your email, click on activation link sent by email and then play with buttons

The server is setup with a timeout of 5 minutes, i.e. if you don't refresh the connection in 5 minutes it disconnects the client.

If you launch the client twice, it will allow just ONE connection at a time, as the license number is set to 1.

Demo license has an 1 month expiration time (configurable too).

Still missing some fancy stuffs, but functionality is almost complete now.

@DOLIK-RCE : could you please test it somehow ?

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by dolik.rce on Thu, 14 Oct 2010 08:30:25 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Thu, 14 October 2010 01:42@DOLIK-RCE : could you please test it somehow ?
I'll try But I'm going to be busy this weekend, so it might take some time.

Also, I will try to update the php version to use the same "protocol". Btw: Still no luck in getting snow2.0 ported to php... If there is someone with spare time and little knowledge of php,, help would be appreciated. The only outcome of my attempts so far is that I actually understood how the cipher works

Honza

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Thu, 14 Oct 2010 08:45:01 GMT
View Forum Message <> Reply to Message

dolik.rce wrote on Thu, 14 October 2010 10:30mdelfede wrote on Thu, 14 October 2010 01:42@DOLIK-RCE : could you please test it somehow ?
I'll try But I'm going to be busy this weekend, so it might take some time.

Also, I will try to update the php version to use the same "protocol". Btw: Still no luck in getting snow2.0 ported to php... If there is someone with spare time and little knowledge of php,, help would be appreciated. The only outcome of my attempts so far is that I actually understood how the cipher works

Honza

Hehehehe.... knowledge is power

Max

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Fri, 15 Oct 2010 08:54:33 GMT
View Forum Message <> Reply to Message

Hello Massimo/Honza

Some questions:

- About Protect

It includes MySql package. Is it possible to remove it?

- About ProtectServer

What are the ProtectServer requirements from server and from client side?.

Is ProtectServer a C++ program running on a server?. What is the role of PHP in this?

Would it be possible to use it with other database instead of MySql?.

Thank you for your work .

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 15 Oct 2010 09:23:38 GMT
View Forum Message <> Reply to Message

koldo wrote on Fri, 15 October 2010 10:54Hello Massimo/Honza

Some questions:

- About Protect

It includes MySql package. Is it possible to remove it?

MySql is needed for ProtectServer, not for the client.
As I made a single package for both (some include files are needed for both cases) the MySql package is needed.... It'll not be linked in cliente, anyways.

Quote:
- About ProtectServer

What are the ProtectServer requirements from server and from client side?.

Is ProtectServer a C++ program running on a server?. What is the role of PHP in this?

ProtectServer requires, by now, an SCGI capable server, so any http server which can support SCGU. I guess almost all servers do. The PHP version that Honza is developing will relax this need.
For apache2 it's enough to install and enable mod_scgi module, and create a small config file for it. For Ubuntu :

sudo apt-get install libapache2-mod-scgi
sudo a2enmmod scgi

And, in /etc/apache2/config.d folder, add an scgi.conf file with this content (as an example) :

SCGIMount /scgi 127.0.0.1:8787

Where the server is listening on port 8787 on local host (configurable) and the http path for it will

be /scgi.

For centos OS it'll just a bit more complicated on step 1, mod_scgi must be manually inserted in apache2.conf.
Anyways, there are many docs on the net to enable SCGI on many http servers... probably I'll add some docs.

ProtectServer is an upp executable. Honza's version will be in PHP and make (maybe) stuffs easier on server side.
Communication is done via encrypted http, so it should pass any routers/firewalls on the way.
ProtectServer NEEDS to run as a daemon / service (it must be continuously running and listening to SCGI port (8787 in my case). It doesn't need to run as root/privileged user.

Quote:
Would it be possible to use it with other database instead of MySql?.

Client is unaware of database type, so the changes are just in server. Honza's PHP is already capable of handling a couple of db engines.
ProtectServer is, by now, tied to MySql, but just because I've no time/no other db engine installed on my server. Adding Postgresql, MSSQL and others should be trivial, as long as they're supported by Upp sql engines.

Quote:
Thank you for your work .

You're wellcome
Please test it, It's setup on my server, you just need to build and run the client. I've still a nasty bug which makes it crash sometimes, but just in devel mode, not in debug builds... so I still didn't caught it.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Fri, 15 Oct 2010 10:05:00 GMT
View Forum Message <> Reply to Message

Hello Massimo

Sorry for the petitions...

I think MySql would have to be removed from Protect, and included only if MySql is explicitly used. In my case I do not use MySql in any case . And now Protect package includes many MySql

elements.

Could you do a basic server version using sqlite, and the possibility to extend it to other databases?. As I do not expect many clients running out there , with sqlite should have to be enough.

What is the advantage of a PHP version if C++ one works?

Quote:Please test it, It's setup on my server
For now with MySql in Protect, I cannot use it, and I really want it .

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 15 Oct 2010 10:23:53 GMT
View Forum Message <> Reply to Message

koldo wrote on Fri, 15 October 2010 12:05Hello Massimo

Sorry for the petitions...

I think MySql would have to be removed from Protect, and included only if MySql is explicitly used. In my case I do not use MySql in any case . And now Protect package includes many MySql elements.

Could you do a basic server version using sqlite, and the possibility to extend it to other databases?. As I do not expect many clients running out there , with sqlite should have to be enough.

What is the advantage of a PHP version if C++ one works?

Quote:Please test it, It's setup on my server
For now with MySql in Protect, I cannot use it, and I really want it .

Mhhhh... what's your problem about including MySql ? It's for the library linking ? It shouldn't be linked anyways for client, just for server.

If your problem is about compiling the server, yep... I could do it. But you could do it also, the *only* files on which the database stuff is used (and encapsulated) are ProtectDB.h/ProtectDB.cpp.
It should be quite easy to add sqlite implementation there.
If you can't / have no time to do it, I can try on this week end.

Last thing... the engine is still missing some cosmetics and a major hardening. By now a malicious client could record a client/server communication (even if it can't decrypt it...), and replay it on the client side to unlock the app.
The solution is quite simple but I haven't implemented yet.
It will be done by passing a random number from/to server, so the replayed communication will be useless.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sun, 30 Jan 2011 18:24:42 GMT
View Forum Message <> Reply to Message

Protect package :

- Fixed a dumb bug on encryption key (Cypher package)

- Refactored Client/Server stuffs, now an authorization key is sent by email in order to activate software on a PC

- Made connection expiration mechanics less sensitive to app crashes on client side.
Now if application crashes, on next run it won't say "license number exceeded" anymore.

- connections not refreshed on give time (default, 5 minutes) will expire on server side; this avoids auth on client side
just on app startup (avoids tricks with hibernations on PC)

Features :

- Product registration; defaults with a timed demo of 1 month

- Settable number of licenses per registered email

- Settable expiration date

- Collects statistics about number of connections per client and total time (seconds) of connections.

- Uses a simple mysql database on server side

- Client/Server communication is encrypted on both sides so it's virtually impossible to fake the authentication

- Allow usage on multiple machines, limited by number of licenses. Once a machine disconnects, it's license is available for another one.

- Returns a key (given on server side) useable with protect code encryption package.

There are still no docs for Client/Server stuffs, but ProtectServerDemo and ProtectClientDemo are quite well commented and shows almost all features

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 04 Feb 2011 00:39:23 GMT
View Forum Message <> Reply to Message

Protect main encryption routines PROTECT_XXX works (finally !!!) with optimized mode in GCC too.... it was quite difficult

OBFUSCATE_xxx macros STILL DON'T WORK in optimized mode, so don't use them or the app will crash
I'm trying to solve it, but not sure that it's possible.

BTW GCC, besides the nasty optimizer that is on the way even if you don't want it, has a nasty bug on __attribute((optimize(0)))
for functions that makes it call wrong ones sometimes, so for now don't do function-level optimizations.
I've seen that also optimization-by-module has sometimes (often...) undesiderable and nasty side effects, so... keep it global !

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 04 Feb 2011 11:04:20 GMT
View Forum Message <> Reply to Message

Now fully working in optimized mode too, both PROTECT and OBFUSCATE macros.
Tested on GCC 4.4.xxx and MSC9.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Apr 2011 08:02:53 GMT

Hi Max,

I tried the ProtectTest package on Windows. It worked beautifully when compiled with MSC9 but crashed when compiled with MSC10. Can you help?

(Also it turns out that 64-bit versions can not be compiled at all. However, this is not currently especially important for me.)

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Apr 2011 11:49:25 GMT

Tom1 wrote on Wed, 06 April 2011 10:02Hi Max,

I tried the ProtectTest package on Windows. It worked beautifully when compiled with MSC9 but crashed when compiled with MSC10. Can you help?

(Also it turns out that 64-bit versions can not be compiled at all. However, this is not currently especially important for me.)

Best regards,

Tom

Hi Tom,

I've just tested it and developed on windows32, MSC9 and on gcc (should work on both 32 and 64 bit of gcc).
The code is STRONGLY dependent on compiler's optimizations, so it's not easy to make it generic.
I've no time right now to test with MSC10, you can do it looking at the generated code; it's not so easy, indeed.
I had the same prolem with GCC in unoptimized vs. optimized mode; on latter the compiler rearranges the code.
On MSC9 there was no difference between optimized and un-optimized; probably MSC10 does it better.
Try to disable optimizations; if it works, you'll have an hint !

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Apr 2011 13:23:33 GMT
View Forum Message <> Reply to Message

Max,

It turns out disabling optimizations on MSC10 does not help in any way. (Maybe you can take a look at it sometime in the future??)

Now, I have a question: After reading the Protect documentation I was left with the impression that OBFUSCATE_START_FUNC and OBFUSCATE_END_FUNC should surround the code used to obtain the key in order to hide the key retrieval details. Well, I tried this modification with the ProtectTest sample application:

```
String GetKey(void)
{
 OBFUSCATE_START_FUNC;
 String key(ScanHexString("AABBCCDDEEFF00112233445566778899"));
 OBFUSCATE_END_FUNC;
 return key;
}
```

... and I got a crash. So, I must have misunderstood something vital. Can you tell me what did I do wrong here?

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Apr 2011 21:18:42 GMT
View Forum Message <> Reply to Message

mhhh... weird. With MSC9 too ?
Anyways, I can't test it right now. Maybe on next days

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Thu, 07 Apr 2011 12:55:06 GMT
View Forum Message <> Reply to Message

Yes, with MSC9.

I kind of found a way around though: First I read the key using obfuscation and store it in a static String variable. Then Decrypt() uses that variable directly when calling PROTECT_DECRYPT(). Then again, I'm not sure if this is really a safe way to do this...(?)

// Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 08 Jun 2011 08:08:48 GMT
View Forum Message <> Reply to Message

Hi Max,

Do you have plans to make the Protect package work on MSC9x64 or MSC10x64? I found out that inline assembly is not supported by Microsoft compilers on x64 architecture, so this may not be easy to solve.

(My application runs out of memory at around 2.4 GB data allocation even with /LARGEADDRESSAWARE linker option, so I need to switch to x64 platform for that app, but still need Protect to work.)

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 08 Jun 2011 08:11:57 GMT
View Forum Message <> Reply to Message

Hmmmmm... I've still not tested MSC9/10 on 64 bit, but if they don't support assembly, we can't do anything about it.
Self decrypting code do need inline assembly.
The only thing I can think about would be to make some modules as 32 bit executables protected with protect and spawned by main app.
Not a very nice solution indeed.....

Max

Edit: thinking about it, it would be maybe possible to write a separate assembly routine which

modify caller code, but that would require quite a bit of work.... If some assembly guru wants to jump into, he's wellcome

---

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Mon, 17 Oct 2011 19:24:49 GMT
View Forum Message <> Reply to Message

Added SQLITE support to Protect packages so that now it is not necessary to have MySQL installed to have the package scrambling and encryption features .

Subject: Re: Protect package - A starting copy protection system
Posted by ratah on Wed, 28 Dec 2011 09:54:21 GMT
View Forum Message <> Reply to Message

Hello everybody,

I try to use Protect package with MingW on Windows but it seems it does not support assembler.

Here is my code

```
/*#include <CtrlLib/CtrlLib.h>
#include <Protect/Protect.h>

using namespace Upp;

void decrypt(byte *start, size_t len, byte const *nonce, size_t nonceLen)
{
   return PROTECT_DECRYPT( start, len,
"\xAA\xBB\xCC\xDD\xEE\xFF\x00\11\x22\x33\x44\x55\x66\x77\x88\x99", nonce, nonceLen);
}

void MyEncryptedFunction()
{
 PROTECT_START_FUNC(decrypt);
  PromptOK("solved");
 PROTECT_END_FUNC;
}

GUI_APP_MAIN
{
 ON_PROTECT_BAD_KEY(decrypt)
 {
    PromptOK("License error");
    exit(1);
 }
```

```
 MyEncryptedFunction();
}
*/

#include <CtrlLib/CtrlLib.h>

#include <Protect/Protect.h>

using namespace Upp;

String GetKey(void)
{
 return ScanHexString("AABBCCDDEEFF00112233445566778899");
}

void Decrypt(byte *start, size_t len, byte const *nonce, size_t nonceLen)
{
 PROTECT_DECRYPT ( start, len, GetKey(), nonce, nonceLen );
}

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;
}

double ObfuscatedTest(double d, double e)
{

 // WARNING -- DON'T PUT ANY return STATEMENT BETWEEN
 // OBFUSCATE_START and OBFUSCATE_END
 OBFUSCATE_START_FUNC;

 double f;
 f = d * e;

 PromptOK("ObfuscatedTest DEOBFUSCATED SUCCESFULLY!!!");

 OBFUSCATE_END_FUNC;
```

```
 return 2 * f + e;
}

GUI_APP_MAIN
{
 ON_PROTECT_BAD_KEY(Decrypt)
 {
  bool res = PromptYesNo("Bad key !!&Do you want to continue anyways ?");
  if(!res)
   exit(0);
 }

 double d = CryptedTest(3, 4);

 d = ObfuscatedTest(3, 4);
 d = ObfuscatedTest(3, 4);

 PromptOK("FINISHED OK !!");

}
```

Here is the error

Do you have an idea?

Thanks and Best wishes for the New year 2012.

Ratah

File Attachments

1) bug.jpg, downloaded 715 times

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Wed, 28 Dec 2011 12:04:22 GMT
View Forum Message <> Reply to Message

Hello Ratah

I have just re-tried package ProtectTest compiled with MinGW 4.5.2 and works well.

In my case it cannot be debugged and the linker gives some warnings about "duplicate section", but the program runs well in XP.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 01 Jun 2018 09:33:30 GMT
View Forum Message <> Reply to Message

Hi all! :)

I'm (finally) trying to update the Protect package, just to solve some of its bugs.
I hope I will succeed, it's not an easy task.
Just some anticipations:

1) It will not use inline assembly code anymore, just a couple of builtins functions available both on GCC and on MSC.
2) It will encrypt ONLY the first byte of each instruction, skipping any address part which may be fixed by linker making
the application crash
3) It should work both for 32 and 64 bit builds now

For point 2 I had to import XED Intel x86 instruction set encoder/decoder; I'll add it to Bazaar to when ready.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Fri, 01 Jun 2018 13:43:13 GMT
View Forum Message <> Reply to Message

Hi Max!

Sounds great!

At this point I wish to point out that I have noticed some customers having my applications freezing at startup with recent Windows 10 systems. I have used PROTECT with MSC9 all these years and the problems have just emerged a few months ago. Not on all systems though. Just some customers. I'm not sure if it has anything to do with PROTECT or writing code on the fly, since Windows does not complain about anything, but clearly something is happening with Windows... Anyway, I'm in process of making a decision how to proceed from now on, but this announcement of yours gives me new hope!

With this new PROTECT, can you support MSBT17 / MSBT17x64 and current U++ Core with C++11?

I wish you the best of luck to this! :)

Thanks and best regards,

Tom

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.

Subject: Re: Protect package - A starting copy protection system
Posted by koldo on Mon, 04 Jun 2018 06:53:55 GMT
View Forum Message <> Reply to Message

Hi Massimo

Thank you for your efforts.

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Tue, 05 Jun 2018 09:37:20 GMT
View Forum Message <> Reply to Message

Hi Max,

This is excellent news. :) Please let me know when you have the first Windows test release ready.

Thanks and best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Tue, 05 Jun 2018 15:19:07 GMT
View Forum Message <> Reply to Message

Hi Tom,

I'm doing some windows tests (MSC15, 32 bit) and it's working ok.
I'll check it with my protected commerial application and, if all is ok, I'll update the package.
You'll need to make some small changes on your sources (quite small!), but it seems to work perfectly, and
it should work on 64 bit MSC too. No assembly at all inside!
I've not handy a 64 bit MSC, so when I'll post it I'll ask you to do some test!

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Tue, 05 Jun 2018 17:10:21 GMT
View Forum Message <> Reply to Message

Hi!

For some reason, I'm not getting email notifications for this thread... Well, I'll keep polling this thread for more good news!

Thanks,

Tom

Update: And yes! I will absolutely test it as soon as I can and report to you.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Tue, 05 Jun 2018 17:30:14 GMT
View Forum Message <> Reply to Message

I don't get any notification either... if you like I can attach here the packages.

I'm fixing other stuffs on my application (protect unrelated, coming from core changes...) so I'll need a bit
more time to test it with protect.
Would you like to have the package preview ?

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Tue, 05 Jun 2018 18:22:10 GMT
View Forum Message <> Reply to Message

Sure! I'll try it tomorrow!

I have two or three different MSC compilers (x86 and x64) installed along with a quite recent nightly upp build, so I can get some useful coverage on the test. Some documentation on the changes required on my code would be useful too. Do you have working ProtectTest and ProtectEncrypt packages available for easy testing?

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Tue, 05 Jun 2018 18:32:32 GMT
View Forum Message <> Reply to Message

Tom1 wrote on Tue, 05 June 2018 20:22Sure! I'll try it tomorrow!

Do you have working ProtectTest and ProtectEncrypt packages available for easy testing?

Tom

Of course!

I'll attach here the 3 packages.
Let me know if it's all ok for you... by now I'm trying to semi-fix the old web package, as the protect server and my paypal IPN server both rely on it :(
BTW, if you know some other ScgiServer implementation that doesn't rely on old web package you're more than wellcome...

(docs are NOT updated!!!)

File Attachments
1) NewProtectPackage.zip, downloaded 286 times

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Tue, 05 Jun 2018 18:39:50 GMT
View Forum Message <> Reply to Message

Hi again,

I forgot the XED package, you need it for new protect code!

File Attachments
1) Xed.zip, downloaded 219 times

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Tue, 05 Jun 2018 19:08:43 GMT
View Forum Message <> Reply to Message

Thanks Max!

I'll test it tomorrow.

BR,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 06:31:19 GMT
View Forum Message <> Reply to Message

Hi Max,

Here are the results from testing Release builds with different compilers:

Without PROTECT flag:
2 * X = 10
2 * X = 20
S is : Hello
S is : Massimo
<--- Finished in (0:01.40), exitcode: 3221225477 --->
With PROTECT flag:
2 * X = 10
2 * X = 20
S is : Hello
<--- Finished in (0:12.26), exitcode: 3221225477 --->

For protected version, the ProtectTest.log file looks like this:

* C:\upp-11979\out\MyApps\MSBT17x64.Protect\ProtectTest.exe 06.06.2018 09:27:24, user: tom

START DECRYPT
JMP NOT FOUND
START DECRYPT
JMP NOT FOUND
START DE-OBFUSCATE
JMP NOT FOUND
START OBFUSCATE

1. On protected version "S is : Massimo" did not print out.

2. Neither 32-bit nor 64-bit version printed out the encrypted data.

3. Please note the 12 second execution time on protected version. It started out fast but took quite a while to complete.

The behavior was exactly the same with MSVS15, MSVS15x64, MSVS17, MSVS17x64, MSBT17 and MSBT17x64.

I think obfuscation needs some tuning as well as encrypted data processing.

In addition to present-day compiler and U++ support, I'm especially pleased to see that the 64-bit variant is now emerging! Good work Max! :)

Thanks and best regards,

Tom

Update: The 12 second long execution time was revealed in Task Manager to involve running "Windows Error Reporting"... I guess this is some sort of a crash and Windows 10 calls home immediately.

Update2: Data encryption/decryption works OK. The problem is entirely in obfuscation; When both obfuscated calls are commented out, encrypted data prints out OK and exit code becomes zero.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 07:04:40 GMT
View Forum Message <> Reply to Message

Hi Tom,

I just fixed it for multithreading, but on my application it seems to work good.
BTW, I don't use obfuscation on it, just encryption.
Could you please do a couple of tests for me ?

1) comment out all calls besides the FIRST obfuscated() one
2) run it, check if it runs ok and look at log file

3) de-comment also the SECOND obfuscated() call
4) run it again

I'm attaching here the modified files for MT safe version

EDIT: please enable the PROTECT_DEBUG macro, if it's not enabled. You should get the assembly listing of code being encrypted
inside the log file

EDIT2: without the PROTECT flag the data decryption is obviously disabled, you just get an empty string... maybe I could return the
original string.

File Attachments

1) Protect.zip, downloaded 171 times

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 07:30:20 GMT
View Forum Message <> Reply to Message

Hi,

First I applied your MT patched files.

Now calling only 'obfuscated("hello");'
S is : Hello
<--- Finished in (0:12.26), exitcode: 3221225477 --->

So it prints out, but crashes on exit. Log looks like this:

* C:\upp-11979\out\MyApps\MSVS17x64.Protect\ProtectTest.exe 06.06.2018 10:21:40, user: tom

START DE-OBFUSCATE
JMP NOT FOUND
START OBFUSCATE

After enabling both obfuscated -calls I still get:
S is : Hello
<--- Finished in (0:12.43), exitcode: 3221225477 --->

And log looks like this:
* C:\upp-11979\out\MyApps\MSVS17x64.Protect\ProtectTest.exe 06.06.2018 10:25:41, user: tom

START DE-OBFUSCATE
JMP NOT FOUND
START OBFUSCATE

So it crashes again when re-obfuscating the code of first call.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 07:36:38 GMT
View Forum Message <> Reply to Message

hmmmm... the weird is that it prints JMP NOT FOUND when de-obfuscating the first time, and with this it can't
de-obfuscate anything.... please wait, I'll add some dump and re-post the code.
BTW, I also corrected data decrypting, now with no PROTECT flag it just extract the data and returns it.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 07:41:16 GMT
View Forum Message <> Reply to Message

Hi Tom,

here the code with fixed non-protected data extraction and some more debug logs.
Please run JUST one obfuscated() call and drop me the log here

Ciao

Mas

File Attachments
1) Protect.zip, downloaded 192 times

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 08:12:10 GMT
View Forum Message <> Reply to Message

Max,

Here's the log:
* C:\upp-11979\out\MyApps\MSVS17x64.Protect\ProtectTest.exe 06.06.2018 11:10:34, user: tom

START DE-OBFUSCATE

SOME BYTES AROUND HEADER START
-10 - 48
-9 - 8d
-8 - 4c
-7 - 24
-6 - 70
-5 - e8
-4 - fc
-3 - 19
-2 - 03
-1 - 00
00 - e8
01 - f7
02 - 73
03 - 01
04 - 00
05 - e8
06 - f2
07 - 73
08 - 01
09 - 00
10 - e8
11 - ed
12 - 73
13 - 01
14 - 00
15 - e8
16 - e8
17 - 73
18 - 01
19 - 00

JMP NOT FOUND
START OBFUSCATE

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 08:33:54 GMT
View Forum Message <> Reply to Message

Hi Tom,

it seems that on debug mode is working and on release not, on my testing machine.
Please wait, I'll investigate a bit more...

EDIT: I guess that the linker is optimizing out the dummy calls used to identify the protected area. I'll try to fix it

---

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 09:49:09 GMT
View Forum Message <> Reply to Message

Hi Tom,

here the last Protect files.
It should work in all cases now... when you test it, please take note at the ProtectEncrypt log when you build
the test package. It should show the number of encrypted and obfuscated chunks of code and data.

The problem was (as usual...) the Microsoft linker, that threw away the empty functions in release mode, and also
replaced the last function call in a function with a jmp.

Ciao

Max

EDIT : if it tests ok I'll update it on Bazaar!

File Attachments
1) Protect.zip, downloaded 173 times

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 10:16:08 GMT
View Forum Message <> Reply to Message

Max,

32-bit is now OK on all my compilers (MSVS15, MSVS17, MSBT17).

However, regardless of compiler, 64-bit executable crashes now immediately. Here's the MSVS17x64 ProtectEncrypt log on TheIDE compiler console:

Linking...
ProtectTest.exe
ENCRYPTION KEY : aabbccddeeff00112233445566778899
LEN:5 e8 b4 26 03 00 call 0x326b9
LEN:3 8d 04 1b lea eax, ptr [ebx+ebx*1]

```
LEN:4  89 44 24 50                mov dword ptr [esp+0x50], eax
LEN:5  e8 08 2d 00 00              call 0x2d0d
LEN:1  48                        dec eax
LEN:2  8b d8                      mov ebx, eax
LEN:1  48                        dec eax
LEN:6  8d 15 1e 4f 17 00           lea edx, ptr [0x174f1e]
LEN:1  48                        dec eax
LEN:2  8b c8                      mov ecx, eax
LEN:5  e8 e6 41 00 00              call 0x41eb
LEN:1  48                        dec eax
LEN:4  8d 54 24 50                lea edx, ptr [esp+0x50]
LEN:1  48                        dec eax
LEN:4  8d 4c 24 28                lea ecx, ptr [esp+0x28]
LEN:5  e8 37 fb ff ff             call 0xfffffb3c
LEN:1  48                        dec eax
LEN:2  8b d0                      mov edx, eax
LEN:4  0f b6 40 0e                movzx eax, byte ptr [eax+0xe]
LEN:2  84 c0                      test al, al
LEN:2  75 07                      jnz 0x9
LEN:1  44                        inc esp
LEN:4  0f be 42 0f                movsx eax, byte ptr [edx+0xf]
LEN:2  eb 04                      jmp 0x6
LEN:1  44                        inc esp
LEN:3  8b 42 08                   mov eax, dword ptr [edx+0x8]
LEN:2  84 c0                      test al, al
LEN:2  74 03                      jz 0x5
LEN:1  48                        dec eax
LEN:2  8b 12                      mov edx, dword ptr [edx]
LEN:1  49                        dec ecx
LEN:2  63 f8                      arpl ax, di
LEN:1  48                        dec eax
LEN:3  8b 4b 18                   mov ecx, dword ptr [ebx+0x18]
LEN:1  48                        dec eax
LEN:3  8d 04 39                   lea eax, ptr [ecx+edi*1]
LEN:1  48                        dec eax
LEN:3  3b 43 28                   cmp eax, dword ptr [ebx+0x28]
LEN:2  77 0e                      jnbe 0x10
LEN:1  4c                        dec esp
LEN:2  8b c7                      mov eax, edi
LEN:5  e8 11 76 15 00              call 0x157616
LEN:1  48                        dec eax
LEN:3  01 7b 18                   add dword ptr [ebx+0x18], edi
LEN:2  eb 09                      jmp 0xb
LEN:1  48                        dec eax
LEN:2  8b 03                      mov eax, dword ptr [ebx]
LEN:1  48                        dec eax
LEN:2  8b cb                      mov ecx, ebx
LEN:2  ff 10                     call dword ptr [eax]
```

```
LEN:1  90                   nop
LEN:5  80 7c 24 36 00         cmp byte ptr [esp+0x36], 0x0
LEN:2  74 0b                 jz 0xd
LEN:1  48                   dec eax
LEN:4  8d 4c 24 28          lea ecx, ptr [esp+0x28]
LEN:5  e8 61 14 00 00         call 0x1466
LEN:1  90                   nop
LEN:1  48                   dec eax
LEN:6  8d 15 a5 4e 17 00      lea edx, ptr [0x174ea5]
LEN:1  48                   dec eax
LEN:2  8b cb                 mov ecx, ebx
LEN:5  e8 71 41 00 00         call 0x4176
LEN:5  e8 89 25 03 00         call 0x3258e
LEN:5  e8 e4 2b 00 00         call 0x2be9
LEN:1  48                   dec eax
LEN:2  8b f8                 mov edi, eax
LEN:1  48                   dec eax
LEN:6  8d 15 0a 4e 17 00      lea edx, ptr [0x174e0a]
LEN:1  48                   dec eax
LEN:2  8b c8                 mov ecx, eax
LEN:5  e8 c2 40 00 00         call 0x40c7
LEN:4  0f b6 43 0e          movzx eax, byte ptr [ebx+0xe]
LEN:2  84 c0                 test al, al
LEN:2  75 07                 jnz 0x9
LEN:1  44                   inc esp
LEN:4  0f be 43 0f          movsx eax, byte ptr [ebx+0xf]
LEN:2  eb 04                 jmp 0x6
LEN:1  44                   inc esp
LEN:3  8b 43 08             mov eax, dword ptr [ebx+0x8]
LEN:2  84 c0                 test al, al
LEN:2  74 03                 jz 0x5
LEN:1  48                   dec eax
LEN:2  8b 1b                 mov ebx, dword ptr [ebx]
LEN:1  49                   dec ecx
LEN:2  63 f0                 arpl ax, si
LEN:1  48                   dec eax
LEN:3  8b 4f 18             mov ecx, dword ptr [edi+0x18]
LEN:1  48                   dec eax
LEN:3  8d 04 31             lea eax, ptr [ecx+esi*1]
LEN:1  48                   dec eax
LEN:2  8b d3                 mov edx, ebx
LEN:1  48                   dec eax
LEN:3  3b 47 28             cmp eax, dword ptr [edi+0x28]
LEN:2  77 0e                 jnbe 0x10
LEN:1  4c                   dec esp
LEN:2  8b c6                 mov eax, esi
LEN:5  e8 fc 74 15 00         call 0x157501
LEN:1  48                   dec eax
```

```
LEN:3   01 77 18                    add dword ptr [edi+0x18], esi
LEN:2   eb 08                       jmp 0xa
LEN:1   48                          dec eax
LEN:2   8b 07                       mov eax, dword ptr [edi]
LEN:1   48                          dec eax
LEN:2   8b cf                       mov ecx, edi
LEN:2   ff 10                       call dword ptr [eax]
LEN:1   48                          dec eax
LEN:6   8d 15 a3 4d 17 00               lea edx, ptr [0x174da3]
LEN:1   48                          dec eax
LEN:2   8b cf                       mov ecx, edi
LEN:5   e8 6f 40 00 00                  call 0x4074
ENCRYPT RESULTS:
Code sequences      : 1
Data sequences      : 2
Obfuscate sequences : 1
C:\upp-11979\out\MyApps\MSVS17x64.Protect\ProtectTest.exe (3476480 B) linked in (0:03.04)

OK. (0:34.67)
```

The ProtectTest.log looks like this:

```
* C:\upp-11979\out\MyApps\MSVS17x64.Protect\ProtectTest.exe 06.06.2018 13:06:22, user: tom

START DECRYPT
LEN: 5 - e8 b4 26 03 00                 call 0x326b9
LEN: 3 - 8d 04 1b                   lea eax, ptr [rbx+rbx*1]
LEN: 4 - 89 44 24 50                    mov dword ptr [rsp+0x50], eax
LEN: 5 - e8 08 2d 00 00                 call 0x2d0d
LEN: 3 - 48 30 d8                   xor al, bl
LEN: 1 - 5e                         pop rsi
LEN: 1 - 50                         push rax
LEN: 2 - 65 1e                      invalid
LEN: 1 - 6c                         insb
LEN: 1 - a5                         movsd dword ptr [rdi], dword ptr [rsi]
LEN: 3 - 0a 6b 39                   or ch, byte ptr [rbx+0x39]
LEN: 1 - 2f                         invalid
LEN: 1 - fc                         cld
LEN: 1 - 54                         push rsp
LEN: 5 - b8 00 00 af 93                 mov eax, 0x93af0000
LEN: 5 - 2d 24 50 fa 74                 sub eax, 0x74fa5024
LEN: 2 - b0 24                      mov al, 0x24
LEN: 5 - bd 91 37 fb ff                 mov ebp, 0xfffb3791
LEN: 2 - 70 b4                      jo 0xffffffffffffffb6
LEN: 2 - 3b d0                      cmp edx, eax
LEN: 1 - 56                         push rsi
LEN: 3 - 49 40 0e                   invalid
LEN: 1 - 5f                         pop rdi
```

```
LEN: 6 - 12 a3 07 bb f1 be                  adc ah, byte ptr [rbx-0x410e44f9]
LEN: 2 - 8a 0f                             mov cl, byte ptr [rdi]
LEN: 2 - cd 04                              int 0x4
LEN: 3 - f2 7f 42                           bnd jnle 0x45
LEN: 2 - 13 fa                             adc edi, edx
LEN: 1 - f4                               hlt
LEN: 5 - 15 03 7c f1 12                       adc eax, 0x12f17c03
LEN: 2 - 49 ce                              invalid
LEN: 1 - 55                               push rbp
LEN: 4 - 48 23 4b 18                          and rcx, qword ptr [rbx+0x18]
LEN: 2 - 4e aa                              stosb byte ptr [rdi]
LEN: 1 - aa                               stosb byte ptr [rdi]
LEN: 1 - 1e                               invalid
LEN: 2 - 48 f8                             clc
LEN: 3 - 80 28 89                             sub byte ptr [rax], 0x89
LEN: 3 - f0 34 a8                           lock xor al, 0xa8
LEN: 5 - bf 51 11 76 15                        mov edi, 0x15761151
LEN: 4 - 23 4c 80 7b                          and ecx, dword ptr [rax+rax*4+0x7b]
LEN: 9 - a1 69 09 c6 2b 03 3a 92 cb                 mov eax, dword ptr [0xcb923a032bc60969]
LEN: 1 - 6e                               outsb
LEN: 1 - 91                               xchg ecx, eax
LEN: 2 - 77 7f                             jnbe 0x81
LEN: 3 - f2 24 36                             and al, 0x36
LEN: 9 - a0 b5 0b 87 40 4c 24 28 2d                 mov al, byte ptr [0x2d28244c40870bb5]
LEN: 3 - 13 14 00                            adc edx, dword ptr [rax+rax*1]
LEN: 3 - 19 65 f2                            sbb dword ptr [rbp-0xe], esp
LEN: 6 - f3 15 a5 4e 17 00                       adc eax, 0x174ea5
LEN: 2 - df 29                             fild st, qword ptr [rcx]
LEN: 2 - 34 7d                              xor al, 0x7d
LEN: 2 - b0 41                              mov al, 0x41
LEN: 1 - cf                               iretd
LEN: 2 - cd eb                              int 0xeb
```

BTW: Should I use 64-bit ProtectEncrypt to process 64-bit executables or is it OK to use the same 32-bit version as for 32-bit executables? (Now I used 32-bit ProtectEncrypt for 64-bit executables, but that's the way I did before too.)

BR,

Tom

EDIT: Yes, answering my own question: ProtectEncrypt must be 64-bit version for 64-bit executables. Now it works beautifully!!! Congratulations Max! This is an excellent step forward!!! :)

Subject: Re: Protect package - A starting copy protection system

Posted by mdelfede on Wed, 06 Jun 2018 10:31:55 GMT
View Forum Message <> Reply to Message

Ehehehehehh... sorry, I forgot to mention it.
The XED package (the one which decodes X86 instructions...) is configured in ProtectEncrypt for 32 bit on 32 bit build and 64 bit on 64 bit builds. It could be changed, but it's not worth the effort.

So it's all working ? If yes, I'll update the Protect package in Bazaar and drop a note about it!

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 10:32:45 GMT
View Forum Message <> Reply to Message

Max,

One question: Do you know if there is a way to configure the post-link step to use 32-bit ProtectEncrypt for 32-bit executables and 64-bit ProtectEncrypt for 64-bit executables? WIN64 flag does not seem to work for that purpose. (Tried to add separate post-link steps to run correct ProtectEncrypt.exe)

Thanks and best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 10:34:51 GMT
View Forum Message <> Reply to Message

Yes, please do update. I will next try to update my own software to use this new Protect!

Thanks,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 10:42:38 GMT
View Forum Message <> Reply to Message

One more detail: It seems that a 64-bit ProtectEncrypt can correctly process both 32 and 64 bit executables, while 32-bit ProtectEncrypt can only process 32-bit executables.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 10:43:14 GMT
View Forum Message <> Reply to Message

Tom1 wrote on Wed, 06 June 2018 12:32Max,

One question: Do you know if there is a way to configure the post-link step to use 32-bit ProtectEncrypt for 32-bit executables and 64-bit ProtectEncrypt for 64-bit executables? WIN64 flag does not seem to work for that purpose. (Tried to add separate post-link steps to run correct ProtectEncrypt.exe)

mhhh... no, I didn't try it. You could modify the ProtectEncrypt application to take another parameter to configure the XED module with the right size, but then I don't know how to sent this parameter to it.
Maybe Mirek can answer to this question... My knowledge on UPP build environment is quite limited.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 10:44:36 GMT
View Forum Message <> Reply to Message

Tom1 wrote on Wed, 06 June 2018 12:42One more detail: It seems that a 64-bit ProtectEncrypt can correctly process both 32 and 64 bit executables, while 32-bit ProtectEncrypt can only process 32-bit executables.

Uhm... that's possible, I didn't try it.
The problem comes from XED library. I don't know if it can process correctly 32 bit code when configured in 64 bit mode.
Maybe yes.

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 11:32:24 GMT
View Forum Message <> Reply to Message

Hi Max,

I have tried to update Protect on one of my own applications and it seems the ProtectEncrypt gets in trouble somehow.

Is it now forbidden to return; between PROTECT_START_FUNC and PROTECT_END_FUNC?

I recall it was only forbidden in OBFUSCATE before.

Best regards,

Tom

UPDATE: I removed all return;s from between PROTECT_START_FUNC and PROTECT_END_FUNC and now it gets processed properly.
UPDATE2: There is still something strange going on with OBFUSCATE. I replaced all OBFUSCATEs with PROTECT and then it works. This is only true with my own software. The ProtectTest works with both.

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 13:27:10 GMT
View Forum Message <> Reply to Message

Hi Tom,

PROTECT should work also with a return inside the encrypted code... if not, it's possible that the compiler re-arrange the code in some weird way. You should activate debugging both on encrypter and on protect and look what happens.

OBFUSCATE doesn't work with an embedded return, for 2 reasons : first, it uses a Mutex on enter and frees it on exit, and the embedded return misses the mutex release; second (and most important) the end part re-encrypts the code, and must be executed when the function exits.

If you've got some code that makes troubles with both protect or obfuscate please run it activating the 2 debug #define and post it the results... and maybe the encrypter log too.

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Wed, 06 Jun 2018 13:30:46 GMT
View Forum Message <> Reply to Message

Hi,

Every now and then I had occasional problems with ProtectEncrypt regarding both PROTECT and OBFUSCATE and the resulting executable on x64. Then I decided to disable optimizations by going from /O2 to /Od. Then both PROTECT and OBFUSCATE started to work on x64 even in my larger application.

I have now added the following pragma to all my cpp source files using PROTECT and/or OBFUSCATE and it seems to stabilize things for now:

#pragma optimize("tsg", off)

Best regards,

Tom

UPDATE: Yes, return; does indeed still work from within PROTECT, but '#pragma optimize("tsg", off)' is needed to avoid optimization which would break it. Do you think it would be a good idea to include this directly in <Protect/Protect.h> to avoid optimization that can break it?

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Wed, 06 Jun 2018 15:19:04 GMT
View Forum Message <> Reply to Message

Tom1 wrote on Wed, 06 June 2018 15:30Hi,

Every now and then I had occasional problems with ProtectEncrypt regarding both PROTECT and OBFUSCATE and the resulting executable on x64. Then I decided to disable optimizations by going from /O2 to /Od. Then both PROTECT and OBFUSCATE started to work on x64 even in my larger application.

This is probably caused by code rearranged by the optimizer... my code requires that the closing macro code comes AFTER the opening one, inside the executable. If the optimizer swap stuffs it doesn't work

Quote:
I have now added the following pragma to all my cpp source files using PROTECT and/or OBFUSCATE and it seems to stabilize things for now:
#pragma optimize("tsg", off)

you should try disabling single optimizations up to it works. Normal optimizations should be harmless.
My code is quite complex and on GCC works correctly. I still have to test it on MSC, but then only on 32 bit... I don't do 64 bit builds for MSC.

Quote:
UPDATE: Yes, return; does indeed still work from within PROTECT, but '#pragma optimize("tsg", off)' is needed to avoid optimization which would break it. Do you think it would be a good idea to include this directly in <Protect/Protect.h> to avoid optimization that can break it?

Maybe that's a good idea. We should try to find the right optimizations... it would be a pity to disable all of them.

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Thu, 07 Jun 2018 10:26:09 GMT
View Forum Message <> Reply to Message

Hi Max,

It seems to me that it is enough to add:

#pragma optimize("g", off)

(i.e. disable 'global optimizations') to get the correct encryption result and working executables with MSC.

UPDATE: This is needed with both 32-bit and 64-bit MSC.
-

Encryption of large applications does seem to require 32-bit ProtectEncrypt for 32-bit executables and 64-bit version for 64 exes. It is really inconvenient to edit manually the post-link step to switch between 32 and 64-bit versions of ProtectEncrypt. Would it be possible to automatically detect 32-bit and 64-bit executables apart and use the correct mode?

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Thu, 07 Jun 2018 11:16:16 GMT
View Forum Message <> Reply to Message

Hi Max,

Here's the last stretch of ProtectEncrypt with added automatic 32/64 -bit Windows PE machine type detection and respective XED configuration. Works with MSBT17/MSBT17x64 on Windows.

```
 Cerr() << "ENCRYPTION KEY : " << HexString(key) << "\n";

 // loads file into buffer
 String fName = CommandLine()[0];
 if(!FileExists(fName))
 {
  Cerr() << "File '" << fName << "' not found\n";
  return;
 }
 FileIn f(fName);
 dword size = (dword)f.GetSize();
 Buffer<byte>buf(size);
```

```
 f.GetAll(buf, size);
 f.Close();

#ifdef WIN32 // Tom added
 int coffindex=*(unsigned int*)&buf[0x3c];
 unsigned short machine=*(unsigned short*)&buf[coffindex+4];
 switch(machine){
  case 0x14c: //i386
   Cout() << "Processing 32-bit i386 executable\n";
   XED.Set32bitMode();
   break;
  case 0x8664: // AMD64
   Cout() << "Processing 64-bit AMD64 executable\n";
   XED.Set64bitMode();
   break;
  default:
   Cout() << "Unknown executable - Cannot process\n";
   return;
 }

#endif

 // encrypt the application
 CryptBuf(buf, buf + size, key);

 // save the encrypted file
 FileOut fOut(fName);
 fOut.Put(buf, size);

 // sets up exit code
 SetExitCode(0);
```

Please merge, if this looks OK to you.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 08 Jun 2018 09:57:41 GMT
View Forum Message <> Reply to Message

Hi Tom,

patch applied!

Still not sure if apply the optimization patch.
Do you have a (short) example showing that the encrypter doesn't work with optimization enabled ?

Ciao

Max

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Fri, 08 Jun 2018 10:42:52 GMT
View Forum Message <> Reply to Message

Hi Max,

Thanks!

Here's an ELF -extended version of the instruction set detection:

```
 unsigned short machine=0; // Unknown
 if((*(unsigned int*)~buf)==0x464c457f) machine=*(unsigned short*)&buf[0x12]; // ELF machine ID
 else if((*(unsigned short*)~buf)==0x5a4d){ // DOS header
  int coffindex=*(unsigned int*)&buf[0x3c]; // Coff header
  machine=*(unsigned short*)&buf[coffindex+4]; // Machine ID
 }

 switch(machine){
  case 0x03: // x86 ELF
   Cout() << "Processing 32-bit i386 ELF\n";
   XED.Set32bitMode();
   break;
  case 0x3e: // x86-64 ELF
   Cout() << "Processing 64-bit AMD64 ELF\n";
   XED.Set64bitMode();
   break;
  case 0x14c: //i386 PE
   Cout() << "Processing 32-bit i386 COFF/PE\n";
   XED.Set32bitMode();
   break;
  case 0x8664: // AMD64 PE
   Cout() << "Processing 64-bit AMD64 COFF/PE\n";
   XED.Set64bitMode();
   break;
  default:
   Cout() << "Unknown executable - Cannot process\n";
   return;
```

}

My Linux VM running U++ is not quite healthy at the moment, so I could not test this ELF thing immediately, but maybe you can. Anyway, the ELF header info is from:

https://en.wikipedia.org/wiki/Executable_and_Linkable_Format

I can't show my actual code, but I'll see what I can do to demonstrate the optimization issue with a test case.

Thanks and best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Fri, 08 Jun 2018 11:00:24 GMT
View Forum Message <> Reply to Message

Max,

Here's the testcase. Just replace the original 'encrypted' function with the following in your ProtectTest.cpp:

```
int squared(int x){
 PROTECT_START_FUNC(GetCypher);
 return x*x;
 PROTECT_END_FUNC;
}

void encrypted(int x)
{
 PROTECT_START_FUNC(GetCypher);
 Cerr() << "X * X = " << squared(x) << "\n";
 PROTECT_END_FUNC;
}
```

So, ProtectEncrypt fails in both 32 and 64 bit mode, unless you add:
#pragma optimize("g", off)
in ProtectTest.cpp.

Anyway, note that speed and size optimizations can still remain enabled.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Fri, 08 Jun 2018 12:22:33 GMT
View Forum Message <> Reply to Message

Hi Max,

I finally got my Linux VM up and running again. It's Linux Mint 18.3 (a 64-bit platform). The good news is that at least ELF-64 detection now works in ProtectEncrypt.

However, it seems now that ProtectEncrypt fails with my previous testcase regardless of compiler (GCC or CLANG). Setting optimization to -O0 does not help here. I wonder if it does some automatic in-lining of functions... or something else.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Fri, 08 Jun 2018 12:41:12 GMT
View Forum Message <> Reply to Message

Max,

I did some quick testing on my 64-bit Linux platform with GCC and CLANG. The result is that if you change the squared function as follows:

```
int __attribute__ ((noinline)) squared(int x){
 PROTECT_START_FUNC(GetCypher);
 int rc=x*x;
 PROTECT_END_FUNC;
 return rc;
}
```

I.e. move return outside the PROTECT envelope, and add "__attribute__ ((noinline))" to avoid inlining, it will work correctly with both CLANG and GCC.

It will work correctly in CLANG without "__attribute__ ((noinline))" too, but still requires return to be outside the PROTECT envelope.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 08 Jun 2018 15:04:22 GMT
View Forum Message <> Reply to Message

Hi Tom,

first, thank you for your code to identify executable type... I embedded it in ProtectEncrypt.

Second, about inlined functions, optimizer and protect: I think that if the function gets inlined the ProtectEncrypt will not work.
That's not for sure, but normally when a function is inlined it is also re-arranged and probably the protect headers and trailers
go out of sync.
Calling an inlined function from inside e protect block SHOULD work, and also the embedded return should do no harm.
I will test your example to see what happens; mostly the return is replaced by compiler with a jmp to code end, but sometimes the code gets re-arranged by the optimizer. I tried my best to avoid it using volatile data inside dummy calls, but it still may happen.

BTW, I'm still not receiving forum notifications... not for private messages, either.
Probably my account is old and the forum software has some bugs, I don't know.

Ciao

Massimo

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Fri, 08 Jun 2018 21:44:01 GMT
View Forum Message <> Reply to Message

Hi Tom,

Tom1

Here's the testcase. Just replace the original 'encrypted' function with the following in your ProtectTest.cpp:
[codeint squared(int x){
 PROTECT_START_FUNC(GetCypher);
 return x*x;
 PROTECT_END_FUNC;
}

[/code]

This happens because the compiler removes ALL the code after the return statement, as it would

be never executet.
I'm trying to find a workaround, but I guess it'll be not an easy task...

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Sat, 09 Jun 2018 07:49:49 GMT
View Forum Message <> Reply to Message

Hi Max,

It might be safest to just document that 'No returns allowed within PROTECT or OBFUSCATE sections.' It is not very difficult to collect the return codes to the end of the function into a single return statement. That's the way I solved the issue in my code anyway.

Inlining of protected functions must be prevented though, because that will in effect create a PROTECT section within another PROTECT section when both functions are protected.

Best regards,

Tom

Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sun, 10 Jun 2018 19:19:32 GMT
View Forum Message <> Reply to Message

Hi Tom, the problem is NOT the return inside protect, just a return with nothing after.
The compiler just removes ALL code after last return, because it doesn't get executed.
it should work, for example, in this case:

```
int encrypted(int x)
{
   PROTECT_START_FUNC(GetCypher)
   if(x == 2)
      return 2*x;
   PROTECT_END_FUNC
   return 3*x;
}
```

But NOT in this one:

```
int encrypted(int x)
{
   PROTECT_START_FUNC(GetCypher)
   if(x == 2)
      return 2*x;
```

```
    return 3*x;
    PROTECT_END_FUNC
}
```

Subject: Re: Protect package - A starting copy protection system
Posted by Tom1 on Tue, 12 Jun 2018 18:23:23 GMT
View Forum Message <> Reply to Message

Hi Max,

Sorry for the delay, I'm really busy at work now.

I see your point. I guess there's no way to go around that with e.g. any dummy addition to PROTECT_END_FUNC either. The simplest way for me was to collect the return value to a variable along the way of execution of function and then return that value in the end after PROTECT_END_FUNC. Everything appears to be working with my code, so it's all good now!

I feel you have made great job with this new version of Protect! Thank you very much Max!

Best regards,

Tom