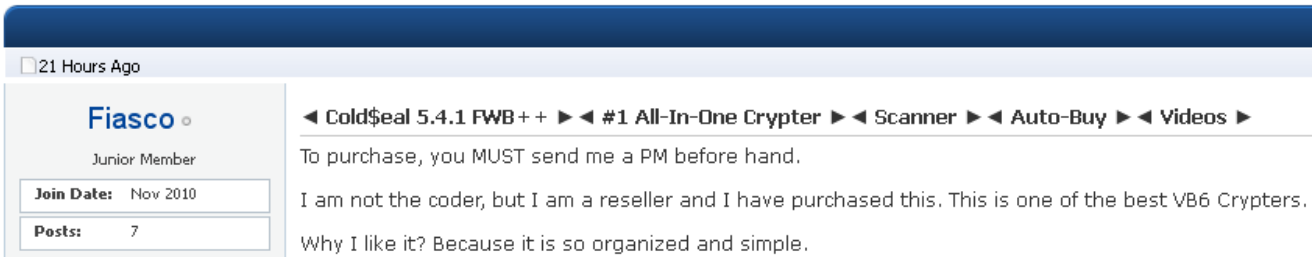
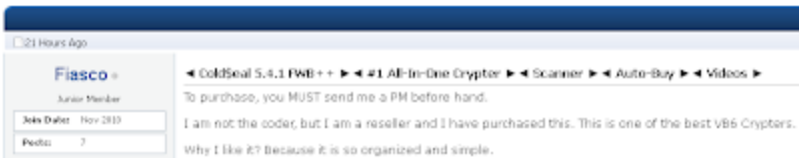
Cracking Cold$eal 5.4.1 FWB++

xylibox.com/2012/01/cracking-coldeal-541-fwb.html



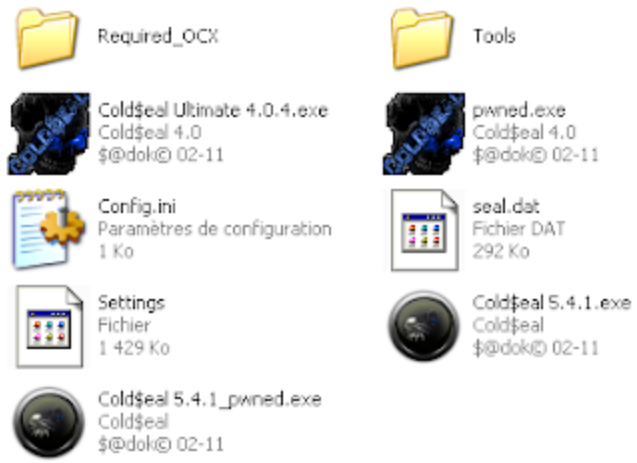
Advert: (Original is on hackforum, but HF seem under heavy DDoS)



Cold$eal is a lame vb6 crypter who use usual crypt tech, they just decorated the GUI to make it “yeahhh”
but really nothing news inside (even on old 4.0 version).

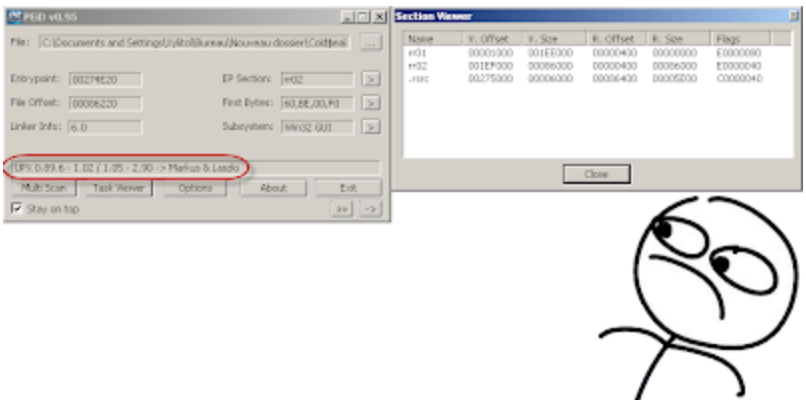
Cold$eal come with a OCX pack, and a folder tools who contain UPX and reshacker.
The author $@dok have forget to remove infos from the tools settings.

31 mars 2011:
D:\Sadok\My Programs\Spynet\Working Runtime crypters\Indetectables Crypter\$@dok's Crypter\Private Release\Cold$eal_IceAge_2011(04.2011)\Tools\Reshacker.exe
D:\Sadok\My Programs\Spynet\Working Runtime crypters\Indetectables Crypter\$@dok's Crypter\Private Release\Cold$eal 4.0\Cold$eal 4.0.exe
C:\Users\$@dok\Desktop\
D:\Sadok\My Programs\Spynet\Working Runtime crypters\Indetectables Crypter\Cold$eal Project\ColdSeal_4.0\Client.vbp
D:\Work\test\4.0\Mouchafer\april\01\Summer_Generated-14\Summer.vbp

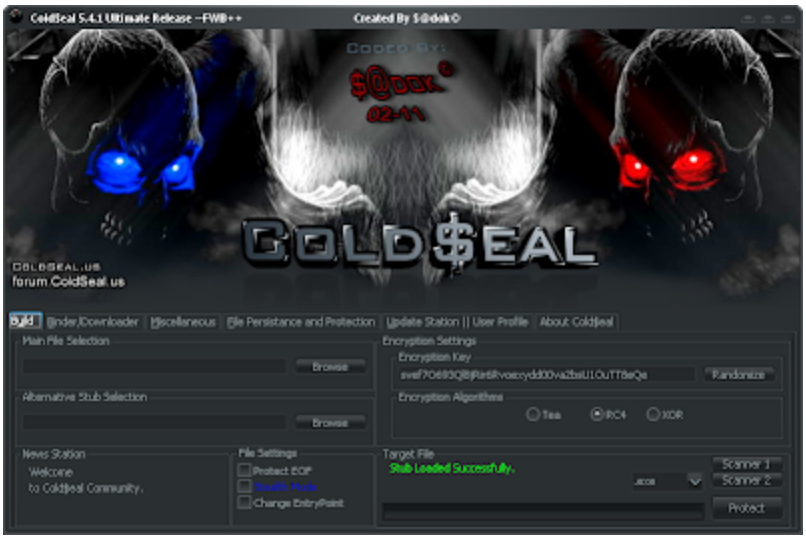


'seal.dat' is the stub.

The builder is packed with a scrambled UPX.



Here is a tiny 'how to' for make it unpackable without firring the debugger:
Rename the sections rr01 and rr02 to UPX0 and UPX1
Then load the file into your favorite hex editor and go to 0x3E0
Remplace the "00" by "UPX!"
Once done: upx.exe -d enjoy.exe (i've told you that come from HF right?)
And then you just have to crack it. (and once again it's vb6, mean if you know the tricks you can do it even without firing a debugger)

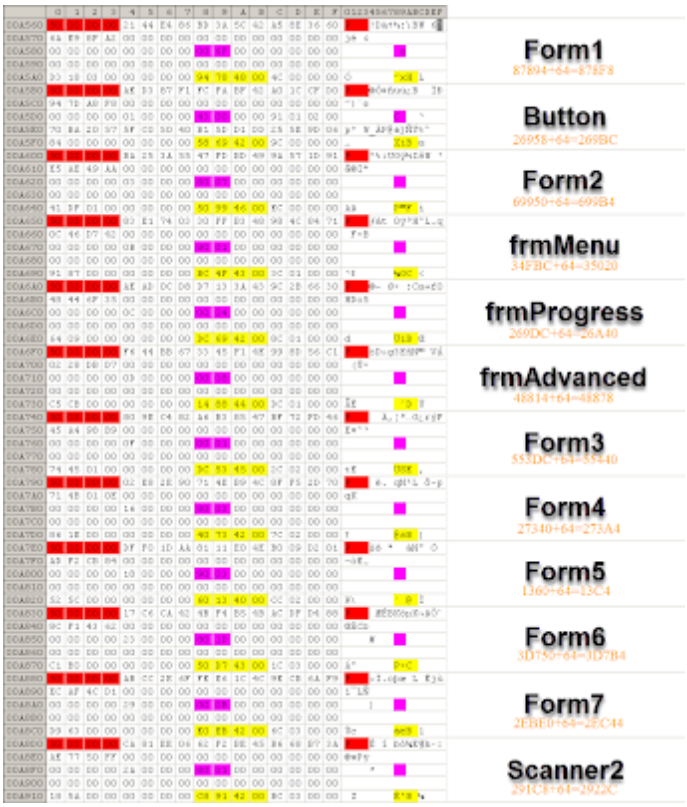


Hmm.. yeah you want to know how, right ?
ok, here we have our typical VB header:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
007600	FC	32	4C	00	F4	F8	4B	00	84	E7	4B	00	BA	9C	41	4C	ü2L ôøK „çK °œAL
007610	00	B9	78	12	40	00	FF	E1	BA	FC	32	4C	00	B9	78	12	¹x @ ÿá°ü2L ¹x
007620	40	00	FF	E1	BA	F4	F8	4B	00	B9	78	12	40	00	FF	E1	@ ÿá°ôøK ¹x @ ÿá
007630	BA	84	E7	4B	00	B9	78	12	40	00	FF	E1	56	42	35	21	°„çK ¹x @ ÿáVB5!
007640	F0	1F	2A	00	00	00	00	00	00	00	00	00	00	00	00	00	ð *
007650	7E	00	00	00	00	00	00	00	00	00	00	00	00	00	0A	00	~
007660	09	04	00	00	00	00	00	00	00	00	00	00	4C	8A	40	00	LŠ@
007670	03	F8	30	01	00	FF	FF	FF	08	00	00	00	01	00	00	00	ø0 ÿÿÿ
007680	0C	00	14	00	E9	00	00	00	60	A5	40	00	A8	11	41	00	é `¥@ ¨ A
007690	A8	12	40	00	78	00	00	00	87	00	00	00	96	00	00	00	¨ @ x ‡ –
0076A0	97	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	—
0076B0	00	00	00	00	43	6F	6C	64	24	65	61	6C	20	35	2E	34	ColdSeal 5.4
0076C0	2E	31	00	43	6F	6C	64	53	65	61	6C	20	35	2E	34	2E	.1 ColdSeal 5.4.
0076D0	31	00	00	43	6F	6C	64	53	65	61	6C	00	01	00	1A	00	1 ColdSeal
0076E0	FC	BB	41	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	ü»A ÿÿÿÿÿÿÿÿ

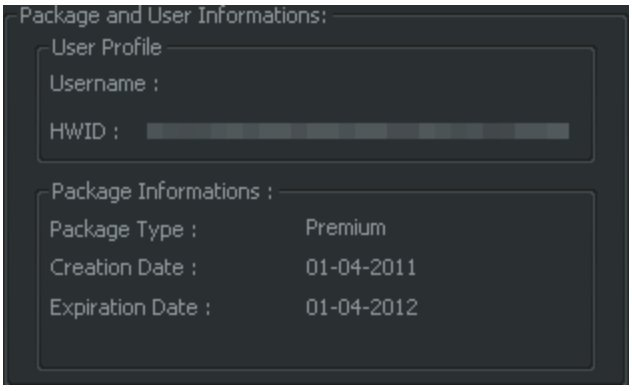
Search for "VB5!" and you will got it.
The information we need is the address of the form header table in yellow, so we go to 0xA560 (Intel format is reversed)

And here we go:



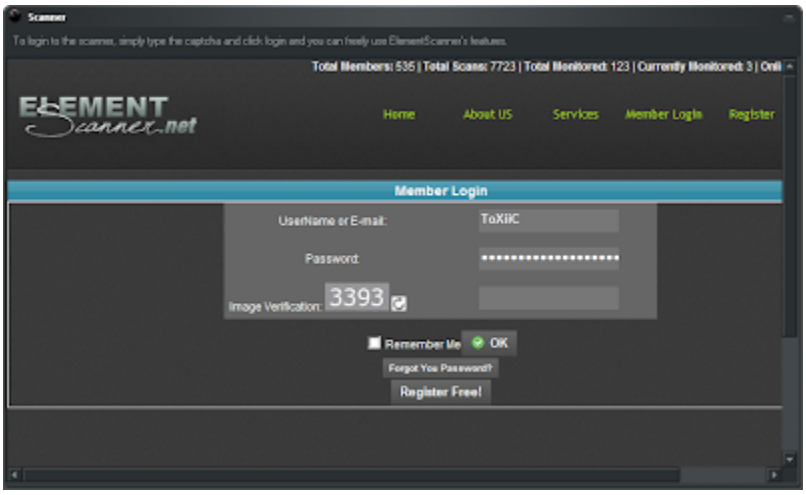
The red part is a delimiter for each form.
the magenta part show the Form attribute
And the yellow part show the Form adress (+ 64h)
We rapidly identify that the HWID check form is "Form5" and the main form is "Form1"

By replacing 006F to 906F on the Form1 attribute and 9003 to 8003 on the Form5 attribute...
Form1 will magically load instead of Form5



Cold$eal Premium and lifetime license for free.

And because you know, everything who come from HF is lame, here is our traditional 'HF faggotry':
Cold$eal have a feature to scan your files on Element Scanner.
So you click on the button and...



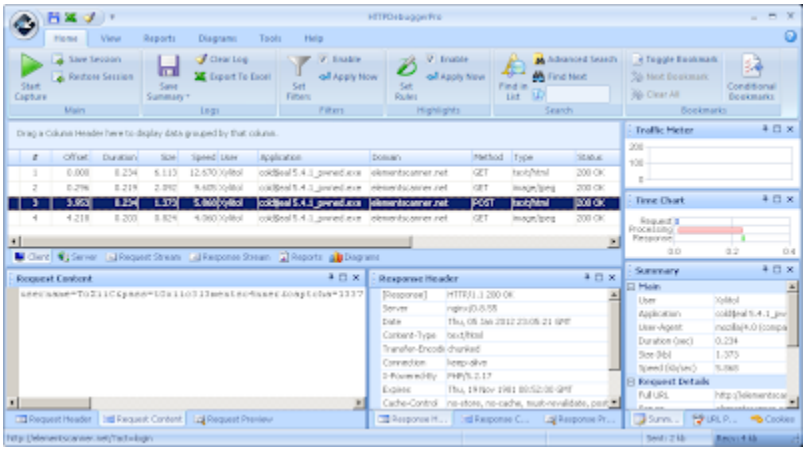
The account and password are pre-typed (LOL)

By simply looking inside the bin or by sniffing the network activity you get the password.

```
UNICODE "http://elementscanner.net/?act=login"

UNICODE "Scanner error:"
UNICODE "Error occured when loading the site. Please try again later."

UNICODE "ToXiiC"
UNICODE "username"
UNICODE "All"
UNICODE "Value"
UNICODE "t0xiic3l3mentsc4nner"
UNICODE "pass"
```



So here you go, free element scanner account:
User: ToXiiC
Password: t0xiic3l3mentsc4nner
Mail: toxiicemail325@yahoo.com

The following urls was found:

• dns: 1 ›› ip: 80.82.65.102 - adresse: COLD-SEAL.NET
http://cold-seal.net/images/
http://cold-seal.net/icons/
http://cold-seal.net/xml/
http://cold-seal.net/cs/

http://cold-seal.net/v2/upload/
http://cold-seal.net/com/mosesSupposes/fuse/
http://cold-seal.net/config/
http://cold-seal.net/auth/
http://cold-seal.net/backgrounds/
http://cold-seal.net/viral/
http://cold-seal.net/www1/www1/
http://cold-seal.net/livesupport/images/
http://cold-seal.net/photoGallery/
http://cold-seal.net/checkuser/
http://cold-seal.net/cgi-bin/
http://cold-seal.net/error/
http://cold-seal.net/phpmyadmin/

• dns: 1 ›› ip: 65.254.248.139 - adresse: ACCOUNTS.COLDSEAL.US
http://accounts.coldseal.us/docs/
http://accounts.coldseal.us/files/
http://accounts.coldseal.us/upload/
http://accounts.coldseal.us/client/
http://accounts.coldseal.us/site/
http://accounts.coldseal.us/stats/
http://accounts.coldseal.us/cpanel/

The following files was found:
http://coldsealus.fatcow.com/Le_PolyTech_Org.pif
http://coldsealus.fatcow.com/coldseal/files/seal.dat
http://coldsealus.fatcow.com/1.exe
http://coldsealus.fatcow.com/coldseal/upload/exe.exe
http://coldsealus.fatcow.com/coldseal/upload/1.exe
http://coldsealus.fatcow.com/coldseal/upload/2.exe
http://coldsealus.fatcow.com/coldseal/upload/4.exe
http://coldsealus.fatcow.com/coldseal/upload/server2.exe
http://coldsealus.fatcow.com/coldseal/upload/44.exe
http://coldsealus.fatcow.com/coldseal/upload/55.exe
http://coldsealus.fatcow.com/coldseal/upload/123.exe
http://coldsealus.fatcow.com/coldseal/upload/svchost.exe

Ah also... you can download Cold$eal and the stub here:
http://accounts.coldseal.us/client/client.rar
http://coldsealus.fatcow.com/coldseal/files/seal.dat

Took 2 sec to brute force..

Or.. no, you can get the archive password from here:
http://accounts.coldseal.us/update.txt

Call that a leak or whatever you want, like it was says on a forum: this is probably the lamest piece of shit i have ever seen.