

# Cracking Cold\$eal 5.4.1 FWB++

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

21 Hours Ago

**Fiasco** ◦

Junior Member

**Join Date:** Nov 2010

**Posts:** 7

◀ Cold\$eal 5.4.1 FWB++ ▶ ◀ #1 All-In-One Crypter ▶ ◀ Scanner ▶ ◀ Auto-Buy ▶ ◀ Videos ▶

To purchase, you MUST send me a PM before hand.

I am not the coder, but I am a reseller and I have purchased this. This is one of the best VB6 Crypters.

Why I like it? Because it is so organized and simple.

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

21 Hours Ago

**Fiasco** ◦

Junior Member

**Join Date:** Nov 2010

**Posts:** 7

◀ Cold\$eal 5.4.1 FWB++ ▶ ◀ #1 All-In-One Crypter ▶ ◀ Scanner ▶ ◀ Auto-Buy ▶ ◀ Videos ▶

To purchase, you MUST send me a PM before hand.

I am not the coder, but I am a reseller and I have purchased this. This is one of the best VB6 Crypters.

Why I like it? Because it is so organized and simple.



**ColdSeal**

**About ColdSeal and the Crew**

ColdSeal is a team of programmers who have coded the best version of the most advanced malware in the world. We are the only team that has been able to create a malware that is so organized and simple that it can be used by anyone. We are the only team that has been able to create a malware that is so organized and simple that it can be used by anyone.

**ColdSeal's Features**

- **Simple and Easy to Use** - ColdSeal is a simple and easy to use malware that can be used by anyone.
- **Advanced Malware** - ColdSeal is a highly advanced malware that can be used by anyone.
- **Organized and Simple** - ColdSeal is a highly organized and simple malware that can be used by anyone.
- **Easy to Install** - ColdSeal is a highly easy to install malware that can be used by anyone.
- **Easy to Run** - ColdSeal is a highly easy to run malware that can be used by anyone.
- **Easy to Hide** - ColdSeal is a highly easy to hide malware that can be used by anyone.
- **Easy to Delete** - ColdSeal is a highly easy to delete malware that can be used by anyone.
- **Easy to Recover** - ColdSeal is a highly easy to recover malware that can be used by anyone.
- **Easy to Update** - ColdSeal is a highly easy to update malware that can be used by anyone.
- **Easy to Patch** - ColdSeal is a highly easy to patch malware that can be used by anyone.
- **Easy to Compile** - ColdSeal is a highly easy to compile malware that can be used by anyone.
- **Easy to Run** - ColdSeal is a highly easy to run malware that can be used by anyone.
- **Easy to Hide** - ColdSeal is a highly easy to hide malware that can be used by anyone.
- **Easy to Delete** - ColdSeal is a highly easy to delete malware that can be used by anyone.
- **Easy to Recover** - ColdSeal is a highly easy to recover malware that can be used by anyone.
- **Easy to Update** - ColdSeal is a highly easy to update malware that can be used by anyone.
- **Easy to Patch** - ColdSeal is a highly easy to patch malware that can be used by anyone.
- **Easy to Compile** - ColdSeal is a highly easy to compile malware that can be used by anyone.



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:

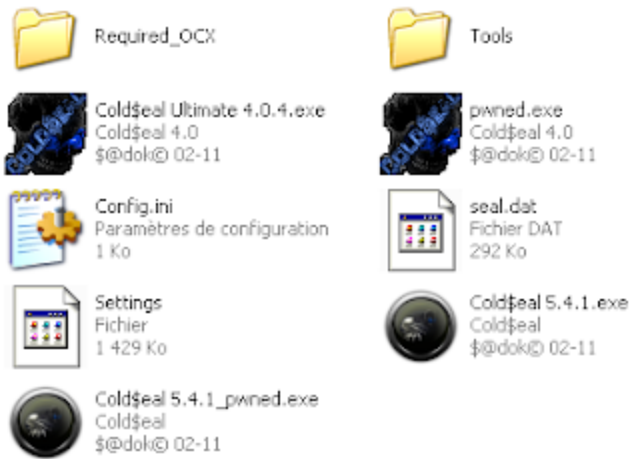
D:\Sadok\My Programs\Spynet\Working Runtime crypters\Indetectables Crypter\@\$dok's Crypter\Private Release\Cold\$eal\_IceAge\_2011(04.2011)\Tools\Reshacker.exe

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

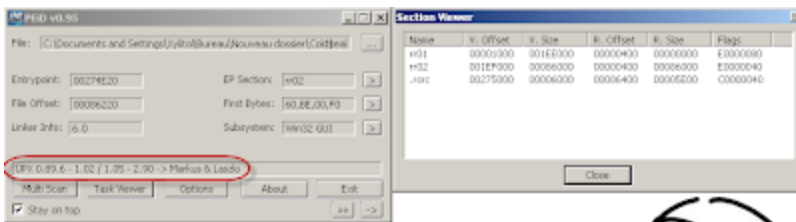
D:\Work\test\4.0\Mouchafer\april\01\Summer\_Generated-14\Summer.vbp



'seal.dat' is the stub.



The builder is packed with a scrambled UPX.



Here is a tiny 'how to' for make it ununpackable 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:

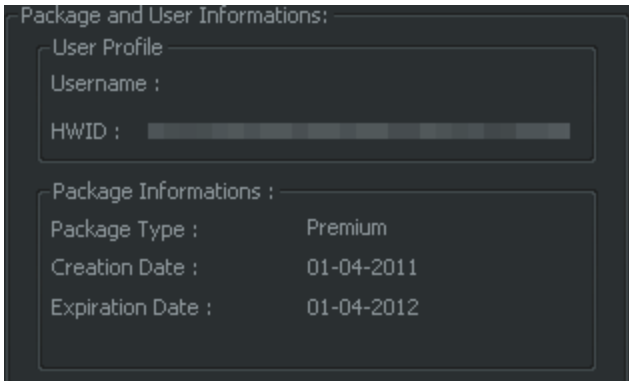
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
007600	FC	32	4C	00	F4	F8	4B	00	84	E7	4B	00	BA	9C	41	4C	u2L 0eK ..qK °eAL
007610	00	B9	78	12	40	00	FF	E1	BA	FC	32	4C	00	B9	78	12	'x @ yá°u2L 'x
007620	40	00	FF	E1	BA	F4	F8	4B	00	B9	78	12	40	00	FF	E1	@ yá°0eK 'x @ yá
007630	BA	84	E7	4B	00	B9	78	12	40	00	FF	E1	56	42	35	21	°..qK 'x @ yáVB5!
007640	FC	1F	2A	00	00	00	00	00	00	00	00	00	00	00	00	00	8 *
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	LS9
007670	03	F8	30	01	00	FF	7F	7F	08	00	00	00	01	00	00	00	e0 yyy
007680	0C	00	18	00	E9	00	00	00	60	A5	40	00	A8	11	41	00	e °00 A
007690	A8	12	40	00	78	00	00	00	97	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	14	ColdSeal 5.4
0076C0	2E	31	00	43	6F	6C	64	53	65	61	6C	20	35	2E	34	1E	! ColdSeal 5.4!
0076D0	31	00	00	43	6F	6C	64	53	65	61	6C	00	01	00	1A	00	! ColdSeal
0076E0	FC	BB	41	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	U»A YYYYYYYY

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)

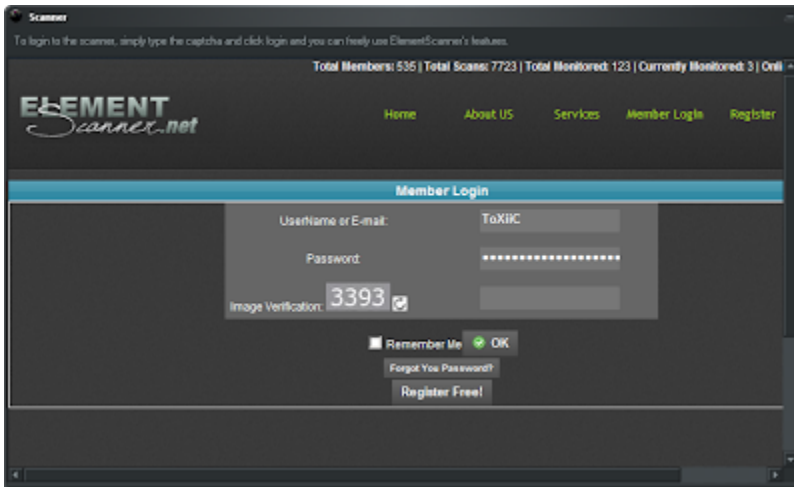
And here we go:

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Comment
EOA550	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form1
EOA554	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	87894+64=87894
EOA558	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Button
EOA55C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	26958+64=26958
EOA560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form2
EOA564	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	69950+64=69954
EOA568	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	frmMenu
EOA56C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	34FBC+64=35020
EOA570	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	frmProgress
EOA574	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	269DC+64=26A40
EOA578	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	frmAdvanced
EOA57C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	48314+64=48378
EOA580	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form3
EOA584	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	553DC+64=55340
EOA588	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form4
EOA58C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	27340+64=273A4
EOA590	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form5
EOA594	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1360+64=13C4
EOA598	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form6
EOA59C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	3D750+64=3D7B4
EOA5A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Form7
EOA5A4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	2EBE0+64=2EC44
EOA5A8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Scanner2
EOA5AC	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	291C8+64=292AC

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...



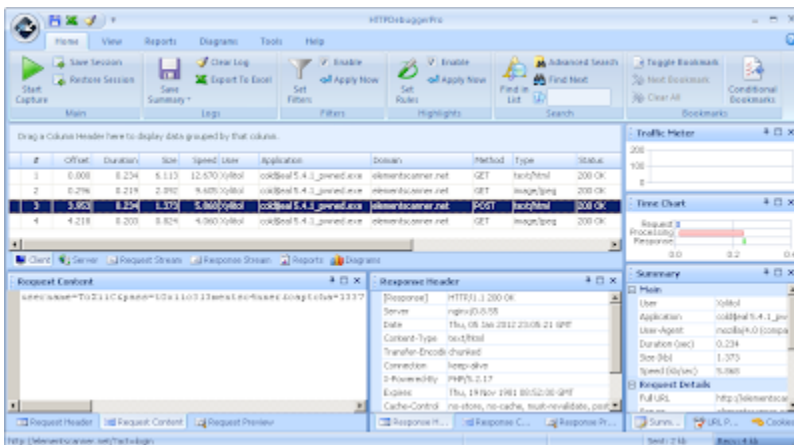
The account and password are pre-typed (LOL)

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/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.