Cracking Cold\$eal 5.4.1 FWB++

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

21 Hours Ago	
Fiasco ∘	Cold\$eal 5.4.1 FWB++ ▶
Junior Member	To purchase, you MUST send me a PM before hand.
Join Date: Nov 2010	I am not the coder, but I am a reseller and I have purchased this. This is one of the best VB6 Crypters.
Posts: 7	Why I like it? Because it is so organized and simple.

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

Fiasco +	◄ ColdSeal 5.4.1 FWB++ ► < #1 All-In-One Crypter ► < Scanner ► < Auto-Buy ► < Videos ►
Junior Member	To purchase, you MUST send me a PM before hand.
Join Date: Nov 2010	I am not the coder, but I am a reseller and I have purchased this. This is one of the best VB6 Crypter
Peda 7	Why I like it? Because it is so organized and simple.

IF I MISEAL IN
About ColdSeal and the Crew Defend was to prevent the two sets of Contents of the set
California and a final statement of the second stateme
ColdSeal's Features
A provide the law day with the second s
In Characteristics and the product of the Accession of the State State
Constant of the local division of the local
et i servere processe and an antipper and a contract of the processes without the processes of the processes
delengen auf delen en er produktionen familieten delen bij
weather restaurated to seed
and a second product of the second product o
Secretary Disc Date AT
THE REAL STREET
And the other and the second sec
Deresting signature (Altheory of Strangenergieses)
Brought space proservices and protection of the
Representationaries and invised in discriment
service and strategy strategies and an end of the service strategies, where
The Older and a strategy of the State of the
And the set of the set
Million Contract Contract
ar or a manufacture of the sector of the sec
have explored as the second end of the second of the secon
Las Areas
Ppenerilillere innersieriersipanitelen Verbins spille, dependenterbiller mannen von
Terresponting and advertising on a Discontinum relation of
The instantian of the second second
in the second state of the
Rama abrele fact and alternative states
The state of the s
WE REALIZED LANDER PROPERTY CONTINUES.
Reservation P
and the second second
had be service the service operator of the
Bandard on anim, identicalise in or. Contracts Marketty and with a descent the
And and the second s



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



Required_OCX



Cold\$eal Ultimate 4.0.4.exe Coldseal 4.0 \$@dok© 02-11



Config.ini Paramètres de configuration 1 Ko



Settings Fichier 1 429 Ko





seal.dat

Tools

pwned.exe

Cold\$eal 4.0

\$@dok© 02-11

Cold\$eal 5.4.1_pwned.exe Cold\$eal \$@dok© 02-11

'seal.dat' is the stub.



The builder is packed with a scrambled UPX.

2 PED v0.95			Section View	ner					. H
Mie: Cilibourents and Settingslystolibue Encrypsint: 002PH220 File Official: 00098220 Linker Entls: 6.0		×	None #01 #02 .ADC	W. Offset 00003300 001EP000 00275000	V. Ste 001EE000 00086000 00006000	R. Offset 00000400 00000400 00000400 00000400	R: Sae	Flags E0000090 E0000040 C0000040	1
[FIF 0.070.6 - 1.12 (1.05 - 2.00 -> Merkus 6. Multi ScanTaak VerwerOptions F Stay on top	About Ed					Close)

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)

ColdSeal 5.4.1 Ultimate Release -FWB++	Created By Silliolato
EBLBEALUS Forum CoklSeatus	Coord Br Soon DLD \$EAL
515 Binder, Downloader Hiscellaneous Ele Persistance an	nd Protection Update Station User Profile About Coldieal
Main Pile Selection	Encryption Settings Encryption Key aver/20693QB/JRdStvoccydd00va2bsU10uTTBeQe Randomize
Alternative Stub Selection	Encryption Algorithms O Tea O RC4 O XOR
Neves Station Pile Settings Welcome Product 2017 to Coldified Community. Charge East	Target File Stale Leaded Successfully Scamer 3 Scamer 2 Protect

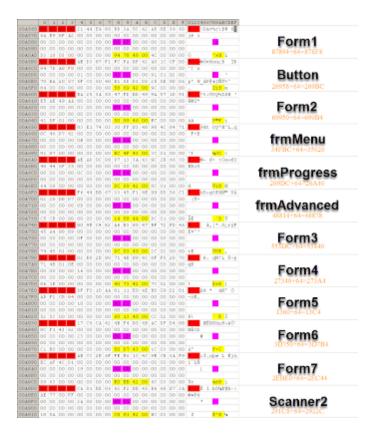
Hmm.. yeah you want to know how, right ? ok, here we have our typical VB header:

• • • • • • • • •			-					יז כי									
	0	1	2	3	-4	5	6	7	8	- 9	Å	В	C	D	E	Ŧ	0123456789ABCDEF
007600	FC	32	4C	00	F4	F8	4B	00	84	E7	4B	00	ВÅ	9C	41	4C	ü2L ösK "ÇK °œàl
007610	00	B9	78	12	40	00	\mathbf{FF}	Ε1	ΒÀ	FC	32	4C	00	B9	78	12	`x 8 ÿá°ü2L `x
007620	40	00	\mathbf{FF}	E1	ΒA	F4	FB	4B	00	B9	78	12	40	00	\mathbf{FF}	Ε1	8 ÿá°ôsK 'x 8 ÿá
007630	Bλ	84	E7	4B	00	В9	78	12	40	00	FF	Ε1	56	42	35	21	°"çK 'x 0 ÿá <mark>VB5!</mark>
007640	FO	1T	2 k	00	00	00	00	00	00	00	00	00	00	00	00	00	6 *
007650	7E	00	00	00	00	00	00	00	00	00	00	00	00	00	ΟÅ	00	~
007660	09	04	00	00	00	00	00	00	00	00	00	00	4C	88	40	00	LŠC
007670	03	F8	30	01	00	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbb{F} \mathbf{F}$	08	00	00	00	01	00	00	00	80 7 77
007680	0C	00	14	00	E9	00	00	00	60	AS	40	00	λ8	11	41	00	é <mark>`¥0</mark> ″X
007690	84	12	40	00	78	00	00	00	87	00	00	00	96	00	00	00	"0x ‡ -
007610	97	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	-
007680	00	00	00	00	43	67	6 C	64	24	65	61	6C	20	35	2E	34	Cold\$eal 5.4
007600	2E	31	00	43	6F	6C	64	53	65	61	6C	20	3.5	2E	34	2E	.1 ColdSeal 5.4.
0076D0	31	00	00	43	6F	6C	64	53	65	61	6C	00	01	00	1λ	00	i ColdSeal
007620	FC	ΒB	41	00	00	00	00	00	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	u»A 99797999

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

-Package and User Inform User Profile	ations:
Username :	
HWID :	
Package Informations	
Package Type :	Premium
Creation Date :	01-04-2011
Expiration Date :	01-04-2012

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':

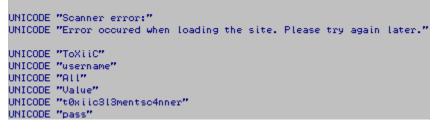
Cold\$eal have a feature to scan your files on Element Scanner.

So you click on the button and...

Scamper					-
	and click login and you can feely use ElementScanner's	leatures.			
	Total Hembers: 535 Total Sca	ansi 7723 Tota	Illenitored: 1	23 Currently Illoni	tored: 3 Onli -
	Home A	vbout US	Services	Member Login	Register
	Member Lo	gin			
	UserName or E-mail:	ΤαΧίΙΟ			
	Password	••••••	•••••		
	Image Verification: 3393 👩				
	Remember Me Forget You Passw Register Fre	forev			

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"



	5 🕱 🛷)•				H	TRO-bugger Fro					_ =)
	fiend .	View	Reports	Diagrams	Tools Help							(
Start Capture	Save Save Sa Restor		Save		Lacel Set Filters	natire opily Now	Set Rules	ly Novi	find in List 😡		Chart Handson (2) Next Dealsman (3) Clear All	Conditional Dockmarks
	Main			Logi	7.83	1	Highlight	2	Seat	dh	Books	
Drag a C	dunn Head	er here to-d	liqley data	proped by that i	duna.						Troffic Histor	+ 🗆 >
	offeet	Duration	Size	Speed Lker	Application	5	osuin	retho	1 Type	1240.6	200	
1	0.000	8.254	6.112	12.6703048sl	okties/5.4.1 gree			GET	hobhtel	200 CH	100	
2	0.276	8.219	2.010	9.405 coltail	coldseal \$14.5 june			OFT	mage/greg	200 CK		
3	3.953	1.254	1.373	5.000 1980	coldinal 5.4.1 gran	d.cos (el	inventocenner .net	POST	bothini	axe ox	Time Chart	+ 🗆 >
-	4.218	8-200	0.824	4.060 Xyleyi	ockSeal 5.4.1_print	den d	ementscorren net.	GET	image/stres	200 OK	Report 1	
1							_				Procelsing Response	
	Server	161 Page	of Stream	Al Fastones 9	ean 🗟 Reports 🧃	Disgram					0.0	0.2 0
-	-						Response Header	_		4 E X	Summary	+ 🗆 >
_	t Canbont				user Loapt dua-						E Hein	1
Leet a	dise-102	arcapae	8-13811	OF THE RESIDENCE OF	unse coalcena.	****		1177/11/1200 (mail:0.858	08.	-	User	10MpC
									112 23 05 21 64		Application	coldeal 5.4.1_pv
								at bind			Liser-Agent:	necilia(4.0 (compa
							Transfer-Encode chi	urked			Duration (sec) See Obl	0.234
							Convector Ne	evilo-qe			Seed (Brive)	1.070
								P/3.2.17		_	E Request Detail	
_									981 80.52.00-9		Full URL	http://www.tecar
						1	Cache-Control ins				ton or	showed as some as
Requ	eet Header	100 Reque	uk Contrent	Request Pr	niew		Response H	Md Rampo	neo C 🖓 A	esponse Pr	📮 Sum 💱	URL P 🧠 Ceokie
		septration is									Sector 7 Mar	Record Man

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/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/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/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/4.exe http://coldsealus.fatcow.com/coldseal/upload/4.exe http://coldsealus.fatcow.com/coldseal/upload/44.exe http://coldsealus.fatcow.com/coldseal/upload/44.exe http://coldsealus.fatcow.com/coldseal/upload/44.exe http://coldsealus.fatcow.com/coldseal/upload/123.exe http://coldsealus.fatcow.com/coldseal/upload/123.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.