



Visagesoft Visual Protect

anorganix of ARTeam

MAY 2006

1.	Brief Introduction	2
2.	Things needed to get started	3
3.	Getting a valid license for VisualProtect	3
4.	Licensing a VP protected Program	5
5.	Making loader for VP and VP protected applications	6
6.	Conclusions.....	7
7.	Greetings.....	7

Keywords

Visual Protect, OllyDbg, HexWorkshop, PEiD



1. Brief Introduction

Visual Protect is a software based protection, e-commerce, and license management tools. With it you can protect any Windows 95/98/NT 32-bit executable from piracy, illegal distribution, and hacking. Protection of your application with Visual Protect requires no source code editing. It allows potential customers to try your complete product before buying, using a simple, smart and user-friendly interface. In addition, thru Visual Protect you can distribute license files to your registered customers as it incorporates a mechanism to manually or automatically generate and send by E-Mail the required registration files.

Visual Protect virtual packaging

Visual Protect Wizard allows you to create a graphical, electronic version of your software packaging. You can easily add graphics, messaging, and Web site links providing the level of detail prospective customers require.

Applying Visual Protect is easy

Once you have completed a software product, you can create a Protection in less than 30 seconds. The Visual Protect Wizard will lead you through a series of steps to include bitmaps, trial parameters, company information and Web site links to automatically create a Protection without changing your source code. Once created, your Protection does not require any modifications for on-line distribution.

Controlled distribution in any format, anywhere

Visual Protect allows you to increase your Web sales and more.

You can electronically distribute Protect-packaged software as trial programs, limited usage offerings and beta tests. Trial periods can be specified to expire on a specific date, after number of uses, or after the expiration of a time period.

Create storefronts and catalogs through the Internet, DVD, CD-ROM or any other digital medium.

Find out more at:

<http://www.visagesoft.com/products/vp/index.php>



2. Things needed to get started

The tools:

Required Tools
<ul style="list-style-type: none">» OllyDbg» PEiD 0.94» HexWorkshop (or other hex viewer/editor)

...and the target:

Target Applications & Protection
<ul style="list-style-type: none">» Visual Protect http://www.visagesoft.com/products/vp/downloads.php

3. Getting a valid license for VisualProtect

Download the program and install it. The first step is to open it in PEiD. Notice that it's protected with itself (Visual Protect » Visage), meaning that the developers of Visual Protect have great confidence in their product... I can't see why... ☺

If you run the target you will see that it's restricted to 15 days and that some options are disabled. As a side note, for those who want to dwell more in this protection I will briefly explain how to reach the OEP, even if we will not need this in our approach.

Fire up Olly and we are here:

Unpacking Visual Protect with Olly		
006BCF90	> 55	PUSH EBP
006BCF91	8BEC	MOV EBP,ESP
006BCF93	51	PUSH ECX
006BCF94	53	PUSH EBX
006BCF95	56	PUSH ESI
006BCF96	57	PUSH EDI
006BCF97	C705 B03E6C00 00000000	MOV DWORD PTR DS:[6C3EB0],0
006BCFA1	68 48206C00	PUSH VisualPr.006C2048

Press Alt+E (Executable Modules) and double-click on VP.dll. Now, right-click and select Search for » All referenced text strings.



Press Ctrl+L and in the search box enter “finalizing” (without the quotes) and make sure that Case sensitive is unchecked and Entire Scope is checked. There will be 2 occurrences of the string, we will double-click on the first.

We arrive here:

Reaching the Target's OEP		
00835FD1	8B8D 58FAFFFF	MOV ECX,DWORD PTR SS:[EBP-5A8]
00835FD7	8D85 5CFAFFFF	LEA EAX,DWORD PTR SS:[EBP-5A4]
00835FDD	BA 946B8300	MOV EDX,VP.00836B94 ; ASCII "Finalizing 0x"
00835FE2	E8 B5E8F5FF	CALL VP.0079489C
00835FE7	8B85 5CFAFFFF	MOV EAX,DWORD PTR SS:[EBP-5A4]
00835FED	E8 46BCFFFF	CALL VP.00831C38
00835FF2	- FF65 FC	JMP DWORD PTR SS:[EBP-4]
00835FF5	6A 00	PUSH 0

Set a breakpoint at 835FDD and hit F9 to run the program. When the nag-screen appears, press the Try button and break in Olly. As you can see ECX holds our OEP. Press F8 a few times, just pass the JMP at 835FF2 and land at the OEP (typical Delphi app):

The Target's OEP		
0066B508	55	PUSH EBP
0066B509	8BEC	MOV EBP,ESP
0066B50B	83C4 F0	ADD ESP,-10
0066B50E	B8 D0AC6600	MOV EAX,VisualPr.0066ACD0
0066B513	E8 E8BCD9FF	CALL VisualPr.00407200
0066B518	A1 34D86700	MOV EAX,DWORD PTR DS:[67D834]
0066B51D	8B00	MOV EAX,DWORD PTR DS:[EAX]
0066B51F	E8 301EE2FF	CALL VisualPr.0048D354
0066B524	A1 34D86700	MOV EAX,DWORD PTR DS:[67D834]
0066B529	8B00	MOV EAX,DWORD PTR DS:[EAX]
0066B52B	BA B0B56600	MOV EDX,VisualPr.0066B5B0

Anyway, a full dump with LordPE is more than enough... Now we need to find the Encryption Key. After dumping, open the file in HexWorkshop and search for the string “visualprotect.vpl”, which is the name of the license file:

Finding the Encryption Key									
0090	CF2B	007B	3736	3539	3644	3243	2D46	...	{76596D2C-F
4445	372D	3434	3345	2D42	3531	442D	3137	DE7-443E-B51D-17	
3034	3432	3839	4442	3538	7D00	0000	0000	044289DB58}.....	
0000	0000	0000	0000	0000	0000	0000	0000	
0000	0000	0000	0000	7670	3130	3000	0000vp100.....	
0000	0000	0000	0000	0000	0000	0000	0000	
0000	0000	0000	0000	0000	0000	0000	0000	
0000	0000	0000	0000	0000	0000	0000	0000	
0000	0000	0000	0000	0000	0000	0000	0000	
0000	0000	0000	0076	6973	7561	6C70	726Fvisualpro	
7465	6374	2E76	706C	0000	0000	0000	0000	tect.vpl.....	

The Encryption Key is just above the license file name, so we got it – it’s “vp100”. Now we have everything we need to generate a license. Launch Visual Protect and select Create a new project. Click Next and set the Expiration date to “01.01.2050”. In the Encryption Key field enter “vp100” (case sensitive) and click Next twice. Under the Protection tab click on Select 32-Bit executable(s)

and then add any executable to the list (make sure that the executable you add is not packed or protected; also rename the executable to “VisualProtect.exe”). Now click on Apply and save the project as “VisualProtect.vpj”. After the program finishes the job, you can close it.

We don't need the packed exe anymore, just keep the new "VisualProtect.vpl" file. Now open the VP help file and click on Licensing » Command Line.

We need to following options:

Command Line Options		
Action	a	"G" or "Generate"
Project	p	Project file name
Register	r	Customer that your product is registered to
Expires	x	Expiration date of registered license (MM.DD.YYYY)

So, fire up Notepad and write the following command:

```

Batch File for License Generation

GLCmd.exe -a g -p visualprotect -r anorganix -x 01.01.2050

^      ^ ^ ^      ^      ^      ^      ^      ^
|      | | |      |      |      |      |      |
|      | | |      |      |      |      |      |
|      | | |      |      |      |      |      +- Expiration date
|      | | |      |      |      |      |      +- Expiration Parameter
|      | | |      |      |      |      |      +- Desired Username for Registration
|      | | |      |      |      |      |      +- Registration Parameter
|      | | |      |      |      |      |      +- Project Name
|      | | |      |      |      |      |      +- Project Parameter
|      | | |      |      |      |      |      +- Generate Parameter
|      | | |      |      |      |      |      +- Action Parameter
|      | | |      |      |      |      |      +- Command Line Program

```

Save the file as “Generate.bat” in the Visual Protect installation folder and launch it. A new license file (called “VisualProtect.vpl”) will be created in the same folder as the exe you protected earlier, thus overwriting the old one. Now replace the “VisualProtect.vpl” (from the VP install folder) with the new one and start the program. Success! The nag is gone and the program is registered...

4. Licensing a VP protected Program

I have included a sample program (protected with VP) in this release. To get a license for it we follow the steps above. Run the program and make a full dump with LordPE. Fire up HexWorkshop and let's look for the Encryption Key. We have to search for "XM.vpl" which is the name of the license file. And we look just above – our Encryption Key is "anorganix@gmail.com".



Finding the Encryption Key

0090	0F0D	007B	3433	3846	3642	4542	2D37{438F6BEB-7
3546	412D	3444	3043	2D39	4544	352D	4335	5FA-4D0C-9ED5-C5
3532	4338	3230	3931	3235	7D00	0000	0000	52C8209125}.....
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	616E	6F72	6761	6E69	7840anorganix@
676D	6169	6C2E	636F	6D00	0000	0000	0000	gmail.com.....
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000XM.vpl...

OK, now to generate a new license for this program. Open Visual Protect and create a new project with Expiration date set to 01.01.2050 (or whatever date you want, but it must be the same as the one in the “Generate.bat” file). Set the Encryption Key and choose any exe for protection. Now edit your batch file and make it look like this:

Batch File for License Generation

```
GLCmd.exe -a g -p XM -r anorganix -x 01.01.2050
```

Launch the batch file and it will generate a new “XM.vpl” file. Overwrite the old one with this new one and start the program. No more nag and no more trial!

5. Making loader for VP and VP protected applications

In some cases, it’s good to know how to bypass this protection scheme with a loader. After studying VP a little I managed to find a place (in every VP protected program) where one instruction patch can make the program registered. Shortly, load the program in Olly and set a breakpoint on the GetSystemDirectoryA API. Press F9, and when Olly breaks hit Ctrl+F9 to execut till return. Then press F8 and you will be back in VP code. Scroll down a little until you can see something like:

Olly View

005553DC	A1 FCBA5500	MOV EAX,DWORD PTR DS:[55BAFC]
005553E1	E8 3ED2FFFF	CALL VP.00552624
005553E6	833D F8BA5500 FF	CMP DWORD PTR DS:[55BAF8],-1
005553ED	0F84 BF000000	JE VP.005554B2
005553F3	33C9	XOR ECX,ECX
005553F5	8B15 FCBA5500	MOV EDX,DWORD PTR DS:[55BAFC]
005553FB	A1 08BB5500	MOV EAX,DWORD PTR DS:[55BB08]
00555400	E8 7FB9FEFF	CALL VP.00540D84
00555405	8BD8	MOV EBX,EAX
00555407	33C9	XOR ECX,ECX
00555409	8B15 00BB5500	MOV EDX,DWORD PTR DS:[55BB00]
0055540F	A1 08BB5500	MOV EAX,DWORD PTR DS:[55BB08]

So, simply NOP the JE at 5553ED and you’re all set. I recommend using loaders for such a job, because in my opinion it’s the “cleanest” way...



6. Conclusions

Well, this is the end of this story, I hope all the things said here will be useful to understand future versions of Visual Protect. I suggest as usual to use this material for learning purposes only, and not for cracking programs. **Thank you for reading this tutorial!**

Disclaimer

All the code provided with this tutorial is free for public use, just make a greets to the authors and the ARTeam if you find it useful. Don't use these concepts for making illegal operation, all the info here reported are only meant for studying and to help having a better knowledge of application code security techniques.

7. Greetings

Thank you Pilli for your support! You are the best!

[ARTeam] [EXETools] [all the RO scene] [bLaCk-eye] [vybez_mR]