PhenoProtect Cracking (Carrera Grand Prix)

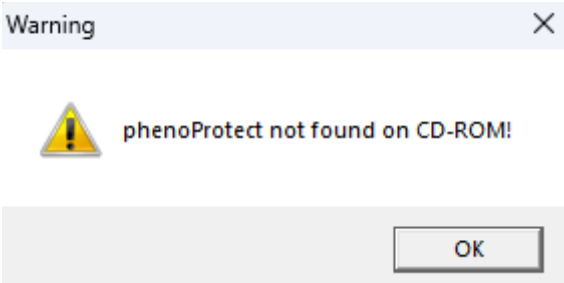
GAME: Carrera Grand Prix [https://www.mobygames.com/game/42347/carrera-grand-prix]
Protection: phenoProtect
Author: Luca D'Amico - https://www.lucadamico.dev - V1.0 - 09-Jun-2024

DISCLAIMER:
All information contained in this technical document is published for general information purposes only and in good faith. Any trademarks mentioned here are registered or copyrighted by their respective owners.
I make no warranties about the completeness, correctness, accuracy and reliability of this technical document. This technical document is provided "AS IS" without warranty of any kind. Any action you take upon the information you find on this document is strictly at your own risk. Under no circumstances I will be held responsible or liable in any way for any damages, losses, costs or liabilities whatsoever resulting or arising directly or indirectly from your use of this technical document. You alone are fully responsible for your actions.

You will need:
- Windows 10/11 VM
- sid installshield script decompiler [https://github.com/tylerapplebaum/setupinxhacking]
- UniExtract v2 [https://github.com/Bioruebe/UniExtract2]
- x64dbg (x32dbg) [https://x64dbg.com/]
- WinCDEmu [https://wincdemu.sysprogs.org/download/]
- Visual Studio Code [https://code.visualstudio.com/]
- d3drm.dll [https://www.dll-files.com/d3drm.dll.html] and DxWnd [https://sourceforge.net/projects/dxwnd/] if you are using a recent Windows version
- Original game disc

Before you start:
This is not a good protection as it is easy to bypass, but despite this, I find it very interesting because unlike the other DRM analyzed previously, this one integrates into the game's installation script and not into its executable.
In this document I will explain two different methods to bypass phenoProtect.

Let's begin:
Let's start by inserting the original game disc into the drive and copy ALL the files and folders to a directory of your choice. For example, I created a directory called "CARRERA" on the desktop and copied the entire contents of the CD into it. Make sure you also copy the hidden files.
If we were to create an ISO image now and proceed with the installation, we would get the following error:



At this point we can proceed with METHOD A or METHOD B.

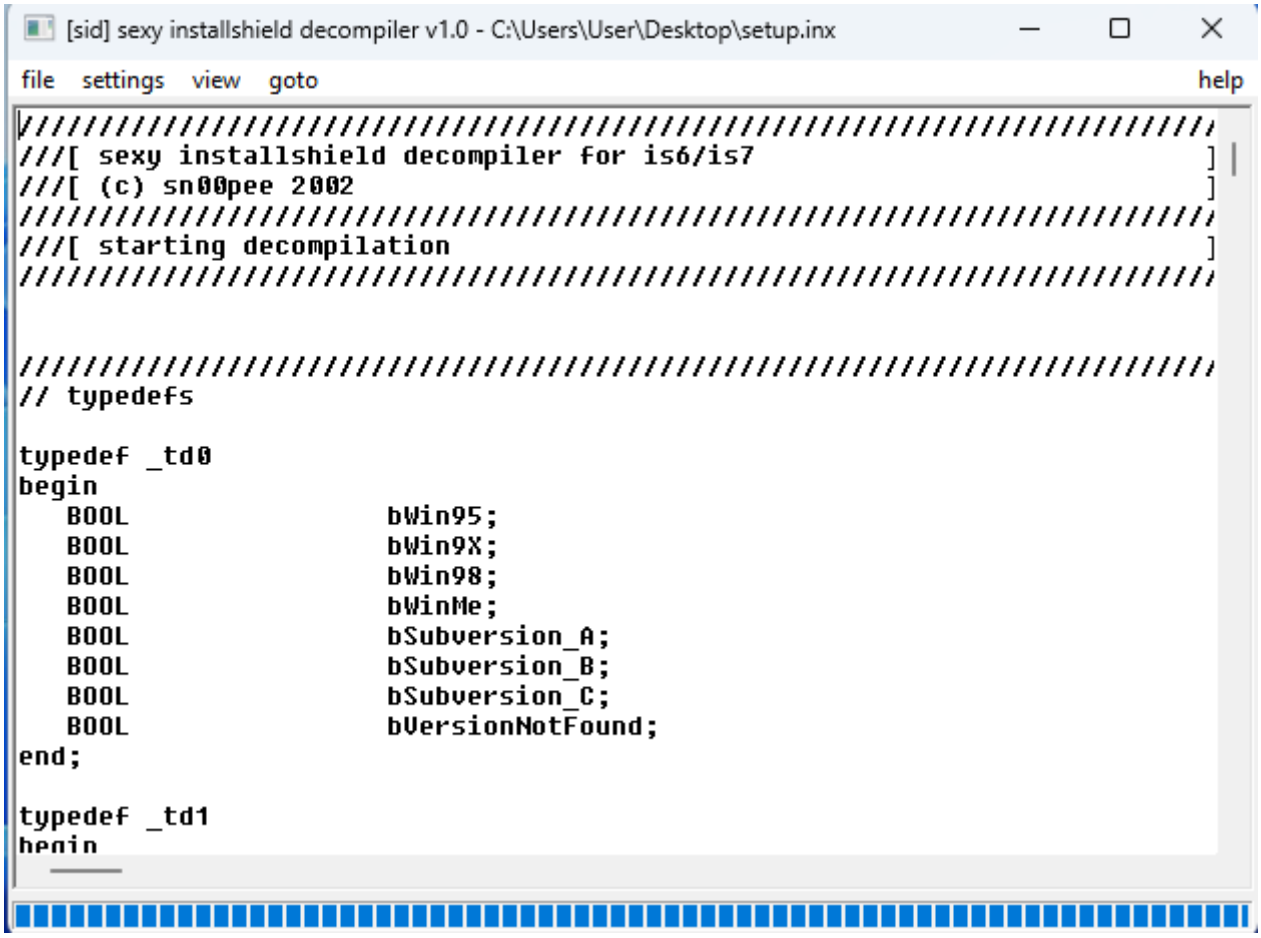
METHOD A:

phenoProtect's check occurs during installation, so this protection has been integrated somehow into the InstallShield script.

This method consists of decompiling this script, called setup.inx, identifying where the check is performed and bypassing it.

To perform the decompilation I used the ‘sexy installshield decompiler' (sid).

Once setup.inx is loaded in sid, we will be provided with the decompiled code:



Unfortunately, this editor is very rudimentary, so for convenience I decided to copy the entire decompiled code into Visual Studio Code.

At this point we can proceed by searching for the error string. We'll get here:

```
892   @00004907:0008   label_4907:
893   @00004909:0021         function_132(4);
894   @00004914:0021         function_398();
895   @0000491A:0006         local_number7 = LASTRESULT;
896   @00004924:000D         local_number7 = (local_number7 = 1036);
897   @00004933:0004         if(local_number7) then // ref index: 1
898   @0000493F:0006            local_string8 = "Recherche du PhenoProtect sur le disque...";
899   @00004973:0006            local_string9 = "PhenoProtect introuvable sur le disque!";
900   @000049A4:0005            goto label_4aae;
901   @000049AD:0007         endif;
902   @000049AD:0007   label_49ad:
903   @000049AF:0021         function_398();
904   @000049B5:0006         local_number7 = LASTRESULT;
905   @000049BF:000D         local_number7 = (local_number7 = 7);
906   @000049CE:0004         if(local_number7) then // ref index: 1
907   @000049DA:0006            local_string8 = "phenoProtect wird auf der CD-ROM gesucht...";
908   @00004A0F:0006            local_string9 = "phenoProtect wurde nicht auf der CD-ROM gefunden!";
909   @00004A4A:0005            goto label_4aae;
910   @00004A53:0002         endif;
911   @00004A53:0002   label_4a53:
912   @00004A55:0006         local_string8 = "Searching CD-ROM for phenoProtect...";
913   @00004A83:0006         local_string9 = "phenoProtect not found on CD-ROM!";
914   @00004AAE:000C   label_4aae:
915   @00004AB0:0021         SetStatusWindow(50, local_string8);
916   @00004ABE:0021         function_132(4);
917   @00004AC9:0021         StatusUpdate(1, 100);
918   @00004AD9:0021         ReadBytes(local_number4, local_string10, 1, 10);
919   @00004AEF:0006         local_number5 = LASTRESULT;
920   @00004AF9:0021         SetStatusWindow(100, local_string9);
921   @00004B07:0021         Disable/Enable(4);
922   @00004B12:000A         local_number7 = (local_number5 > 0);
923   @00004B21:0004         if(local_number7) then // ref index: 1
924   @00004B2D:0021            CloseFile(local_number4);
925   @00004B36:0021            MessageBox(local_string9, -65534);
926   @00004B44:0002            abort;
927   @00004B48:0003         endif;
928   @00004B48:0003   label_4b48:
929   @00004B4A:0021         SeekBytes(local_number4, 40000, 1);
```

The decompiled code is easy to read and understand; we immediately see that a MessageBox is called (at address 00004A83) if the condition at address 00004B21 is satisfied. Reading a few lines above, we notice that the condition is influenced by the return value of the ReadBytes call (at address 00004AD9) and if it is greater than 0 (address 00004B12) then the protection will be triggered displaying the error message and preventing us from installing the game.

For the more curious, we can briefly continue the analysis. We know that the condition triggering the error message is influenced by the return value of the ReadBytes function. The documentation of this API can be found here: https://docs.revenera.com/installshield22helplib/Subsystems/installshield22langref/helplibrary/LangrefReadBytes.htm and therefore, we understand that the script is trying to read 10 bytes from the handle contained in the local_number4 variable.

Going up a few lines of code, we can see that this handle is obtained from the file “DATA2.CAB”:

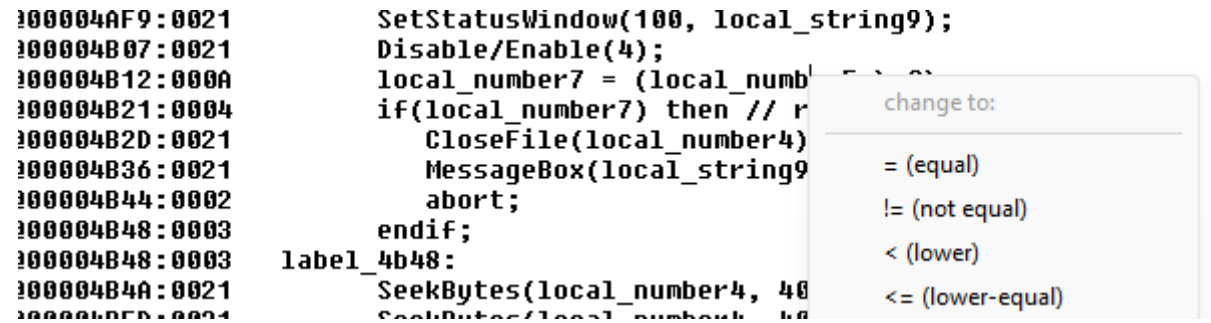
```
local_string6 = "DATA2.CAB";
OpenFile(local_number4, local_string7, local_string6);
```

And right below that, a call is also made to SeekBytes:

```
SeekBytes(local_number4, -40000000, 3);
```

So, we can assume that if it is possible to correctly read 10 bytes from that position (hexadecimal), then the inserted disk is not original.

At this point I would proceed by completely disabling the control, but unfortunately sid only allows us to apply rudimentary patches; therefore, we are forced to invert the logic of the if rather than eliminate it completely. Let's go back to the sid window, right-click on the condition at the address 00004B12, then choose "<= (lower-equal)" from the drop-down menu to invert the logic of the check:



The code will be updated with our patch (a comment will appear saying “// changed to "<=""”).

We can now save our patched script. Let’s click on File, choose “patch changes” and confirm that we want to save the file.

Overwrite the setup.inx file with your modified version (if you haven't already) and create a new ISO image (you can use WinCDEmu) from the previously extracted files.

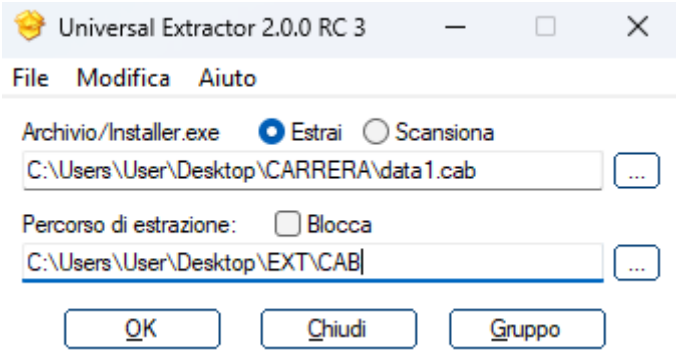
Let's mount the newly created ISO and try to install the game: phenoProtect will no longer block us as the check has been reversed. Great job!

Once you have installed the game, if you are using a recent version of Windows, there may be some compatibility issues. You need to copy the d3drm.dll library into the game installation directory and configure DxWnd to start when the game executable (_crrr.exe) is launched. Everything will work fine.

METHOD B:

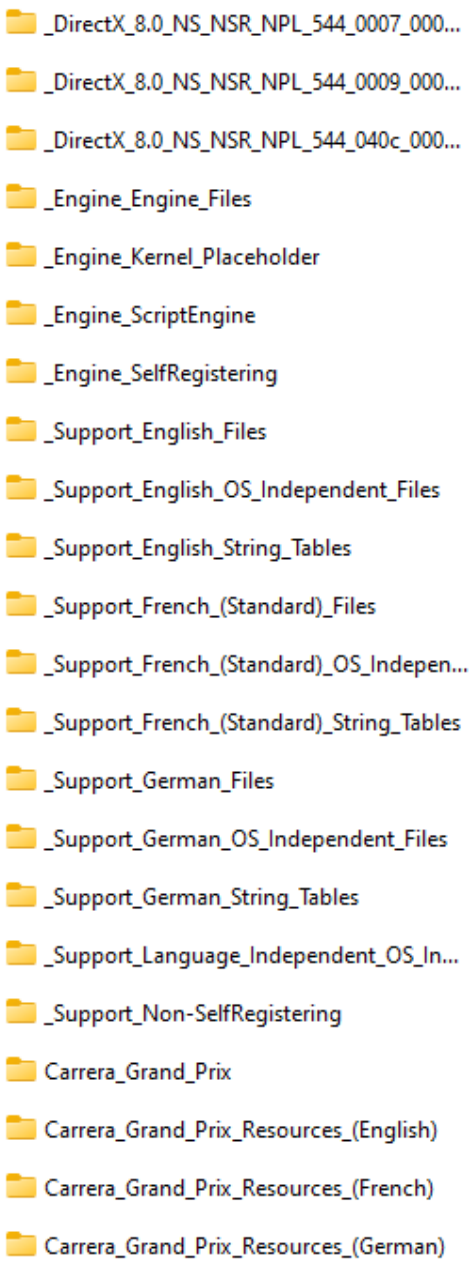
In Method A, we bypassed phenoProtect by modifying the installation script. However, there is a second method: extracting all game files without using the installer.

We can use a tool called UniExtract v2 to unpack the CAB archives present on the game disk and obtain the files. Open UniExtract and choose the data1.cab file:



Extracting the data2.cab file is unnecessary, as UniExtract processes it automatically.

Once the extraction is complete, let's open the destination folder. We will find the following directories:



Let's copy the "Carrera_Grand_Prix" directory, which is the main one, to the desktop and then copy the contents of the "Carrera_Grand_Prix_Resources_(English)" directory (i.e. the ART0001.RFD and ART0001.RFH files) into it. If you are using a recent version of Windows, don't forget to copy the d3drm.dll library downloaded previously and to configure DxWnd to start when _crrr.exe is launched, to avoid compatibility issues.

At this point, launching Carrera.exe will reveal an 'Install' button instead of 'Play'. This is because the game, not finding the relevant keys added to the system registry during installation, believes that it still needs to be installed.

We can proceed in two ways:

- By using x32dbg, setting a breakpoint on RegCloseKey and forcing the conditional jump right after returning to the application code
- By installing the game using Method A and dumping the needed keys from the system registry

Both methods are effective, but if you choose the first one, you will also have to apply some extra patches to disable the cd-check and redirect the loading of the resource.cfg file from the CD-drive to the game's installation folder (at address 00403EBB). Additionally, you will also have to force the conditional jump at address 00403B7F to make the game load the files from the current directory.

If you want to use the second method, you just need to install the game and perform, using regedit, a simple dump of:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Take2\Carrera Grand Prix

Now you can proceed by uninstalling the game. Let's edit the value of the "Path" key from the .reg file (opening it with notepad) replacing the old one with the path of the directory where you extracted the game files, and finally import it into your registry. Start Carrera.exe again from your directory and everything will work correctly. Even in this case, if you want, you can remove the cd-check as described above.

Credits:

I'd like to thank Codecult/Phenomedia AG for creating this unique protection scheme.

A big thank you also goes to the authors of the tools used to perform this analysis.

Conclusion:

This was a very fun protection scheme to analyse, as it is entirely different from those I have documented so far. Its simplicity also makes it perfect for beginners and first-time reversers. It's a shame that it has only been used in a couple of games.

Thank you for reading!

Luca