

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 Giugno 2024

DISCLAIMER:

Tutte le informazioni contenute in questo documento tecnico sono pubblicate solo a scopo informativo e in buona fede.

Tutti i marchi citati qui sono registrati o protetti da copyright dai rispettivi proprietari.

Non fornisco alcuna garanzia riguardo alla completezza, correttezza, accuratezza e affidabilità di questo documento tecnico.

Questo documento tecnico viene fornito "COSÌ COM'È" senza garanzie di alcun tipo.

Qualsiasi azione intrapresa sulle informazioni che trovi in questo documento è rigorosamente a tuo rischio.

In nessun caso sarò ritenuto responsabile o responsabile in alcun modo per eventuali danni, perdite, costi o responsabilità di qualsiasi tipo risultanti o derivanti direttamente o indirettamente dall'utilizzo di questo documento tecnico. Solo tu sei pienamente responsabile delle tue azioni.

Cosa ci serve:

- Una VM con Windows 10/11
- 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>] e DxWnd [<https://sourceforge.net/projects/dxwnd/>] se state usando una versione recente di Windows
- Disco di gioco originale (abbiamo bisogno del disco ORIGINALE)

Prima di iniziare:

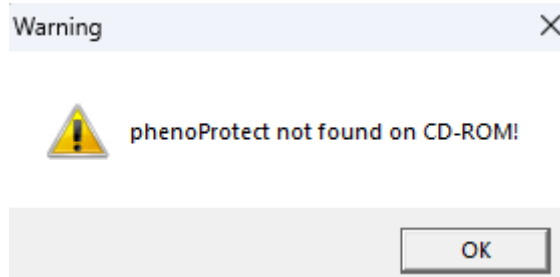
Questa non è una buona protezione ed è facile da bypassare, ma, nonostante ciò, la reputo molto interessante perché a differenza degli altri DRM analizzati precedentemente, questo si integra nello script di installazione del gioco e non nel suo eseguibile.

In questo documento spiegherò due metodi diversi per eludere phenoProtect.

Iniziamo:

Come prima cosa inseriamo il disco del gioco originale nel lettore e copiamo TUTTI i file su una cartella da noi scelta. Ad esempio, io ho creato una cartella chiamata "CARRERA" sul desktop e ho copiato l'intero contenuto del cd dentro di essa. Assicuratevi di copiare anche i file nascosti.

Se creassimo ora una immagine ISO e procedessimo all'installazione, otterremmo il seguente errore:



A questo punto siamo pronti per procedere con il METODO A o con il METODO B.

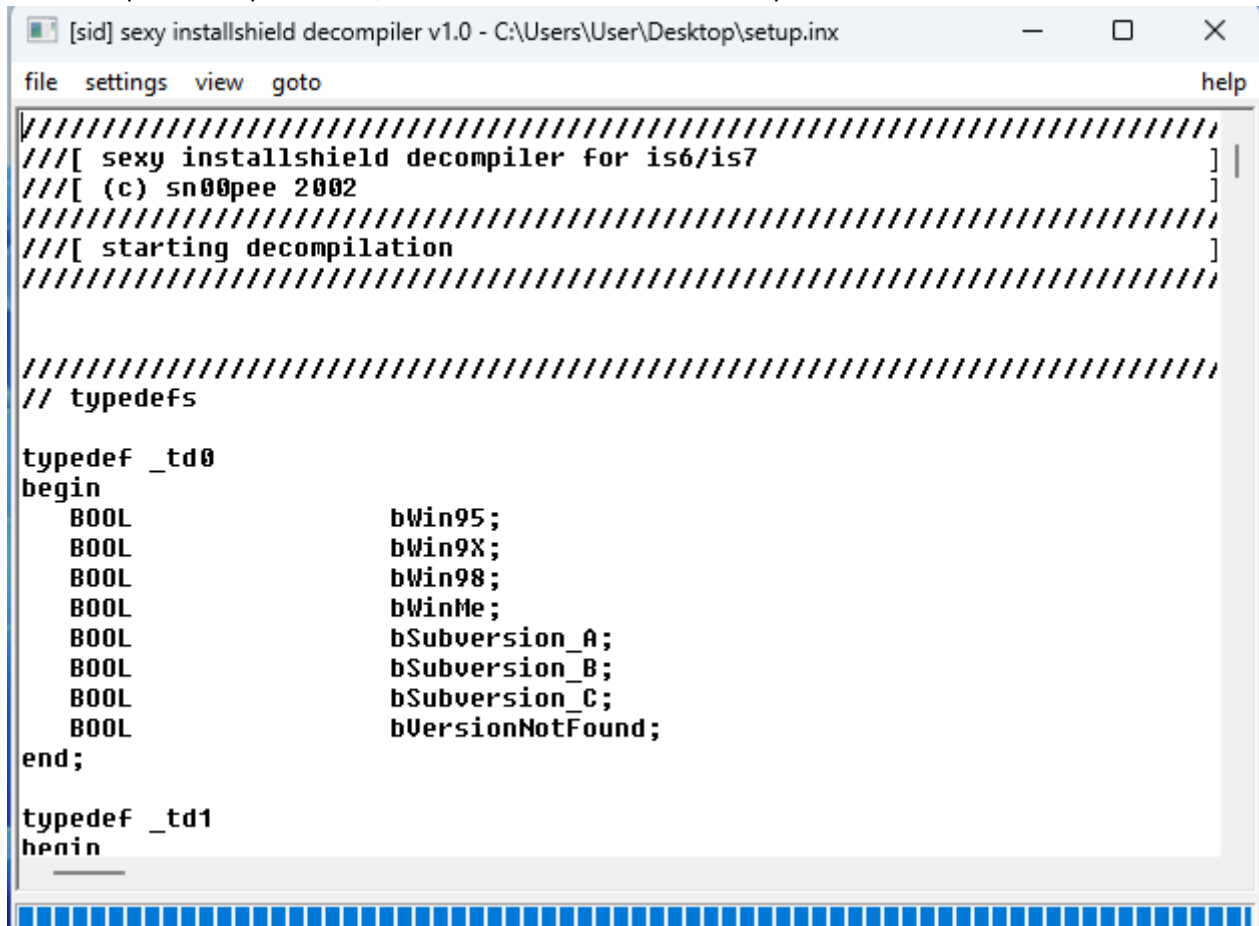
METODO A:

Come possiamo immaginare il controllo effettuato da phenoProtect avviene in fase di installazione, quindi questa protezione è stata integrata in qualche modo nello script di InstallShield.

Questo metodo consiste nel decompilare questo script, chiamato setup.inx, individuare dove viene effettuato il controllo e bypassarlo.

Per effettuare la decompilazione ho usato “sexy installshield decompiler” (sid).

Una volta aperto setup.inx in sid, ci verrà fornito il relativo decompilato:



```
[sid] sexy installshield decompiler v1.0 - C:\Users\User\Desktop\setup.inx
file settings view goto help

////////////////////////////////////
///[ sexy installshield decompiler for is6/is7 ] |
///[ (c) sn00pee 2002 ]
////////////////////////////////////
///[ starting decompilation ]
////////////////////////////////////

////////////////////////////////////
// typedefs

typedef _td0
begin
    BOOL          bWin95;
    BOOL          bWin9X;
    BOOL          bWin98;
    BOOL          bWinMe;
    BOOL          bSubversion_A;
    BOOL          bSubversion_B;
    BOOL          bSubversion_C;
    BOOL          bVersionNotFound;
end;

typedef _td1
begin
```

Purtroppo, questo editor è molto rudimentale, così per comodità ho deciso di copiare tutto il decompilato in Visual Studio Code.

A questo punto possiamo procedere cercando la stringa con il messaggio d’errore. Arriveremo qui:

```

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);

```

Il decompilato è molto facile da leggere e comprendere, infatti vediamo subito che viene chiamata una MessageBox (all'indirizzo 00004A83) qualora la condizione contenuta nell'if (all'indirizzo 00004B21) sia soddisfatta. Leggendo qualche riga più sopra, notiamo che la condizione è influenzata dal valore di ritorno della chiama ReadBytes (all'indirizzo 00004AD9) e se questo è maggiore di 0 (indirizzo 00004B12) allora la protezione scatterà visualizzando il messaggio di errore impedendoci di installare il gioco.

Per i più curiosi, possiamo continuare brevemente l'analisi: sappiamo che il controllo che fa scattare il messaggio d'errore viene influenzato dal valore di ritorno della funzione ReadBytes. La documentazione di questa API la possiamo trovare qui:

<https://docs.revenera.com/installshield22helplib/Subsystems/installshield22langref/helplib/LangrefReadBytes.htm> e quindi possiamo comprendere che lo script sta tentando di leggere 10 bytes dall'handle contenuto nella variabile local_number4. Salendo di qualche riga di codice, possiamo vedere che questo handle corrisponde al file "DATA2.CAB":

```

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

```

E subito sotto viene anche fatta una chiamata a SeekBytes:

```

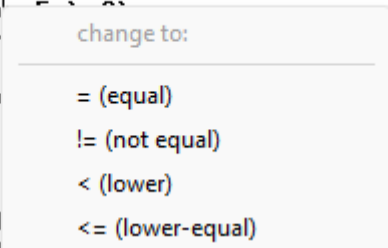
SeekBytes(local_number4, -40000000, 3);

```

Quindi possiamo ipotizzare che se è possibile leggere correttamente 10 bytes da quella posizione (in esadecimale), allora il disco inserito non è originale.

A questo punto procederei disabilitando completamente il controllo, ma purtroppo sid ci permette di applicare solo patch rudimentali; quindi, siamo costretti ad invertire la logica dell'if piuttosto che eliminarla completamente. Procediamo tornando alla finestra di sid e clicchiamo con il dito sulla condizione all'indirizzo 00004B12, dal menu a tendina scegliamo quindi "<= (lower-equal)" per invertire la logica del controllo:

```
00004AF9:0021      SetStatusWindow(100, local_string9);
00004B07:0021      Disable/Enable(4);
00004B12:000A      local_number7 = (local_number7 <= 0);
00004B21:0004      if(local_number7) then // r
00004B2D:0021          CloseFile(local_number4)
00004B36:0021          MessageBox(local_string9, local_string9, MB_OK);
00004B44:0002          abort;
00004B48:0003      endif;
00004B48:0003      label_4b48:
00004B4A:0021      SeekBytes(local_number4, 40, 0);
00004B50:0021      SeekBytes(local_number4, 40, 0);
```



Il codice verrà aggiornato con la nostra patch (apparirà un commento con scritto "// changed to "<="").

Procediamo salvando il nostro script patchato con il controllo invertito: clicchiamo su File, scegliamo "patch changes" e confermiamo di voler salvare il file.

Sovrascrivete il file setup.inx con la vostra versione modificata (se non lo avete già fatto) e creiamo una nuova immagine ISO (potete usare WinCDEmu) con i file estratti precedentemente.

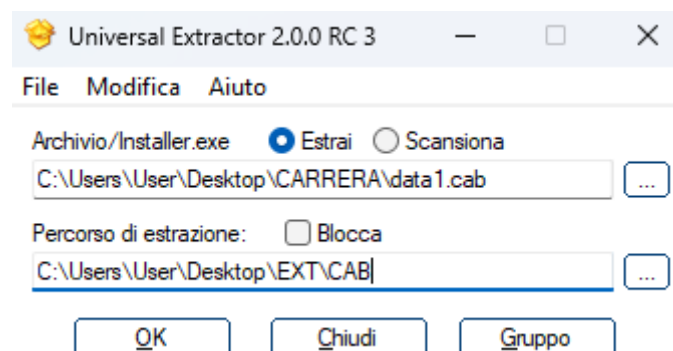
Montiamo la ISO appena creata e proviamo ad installare il gioco: phenoProtect non ci bloccherà più in quanto il check è stato invertito! Ottimo lavoro!

Una volta installato il gioco se state usando una versione recente di Windows potrebbero esserci dei problemi di compatibilità. Occorre copiare la libreria d3drm.dll nella cartella di installazione ed impostare DxWnd sull'eseguibile _crrr.exe. Tutto funzionerà correttamente.

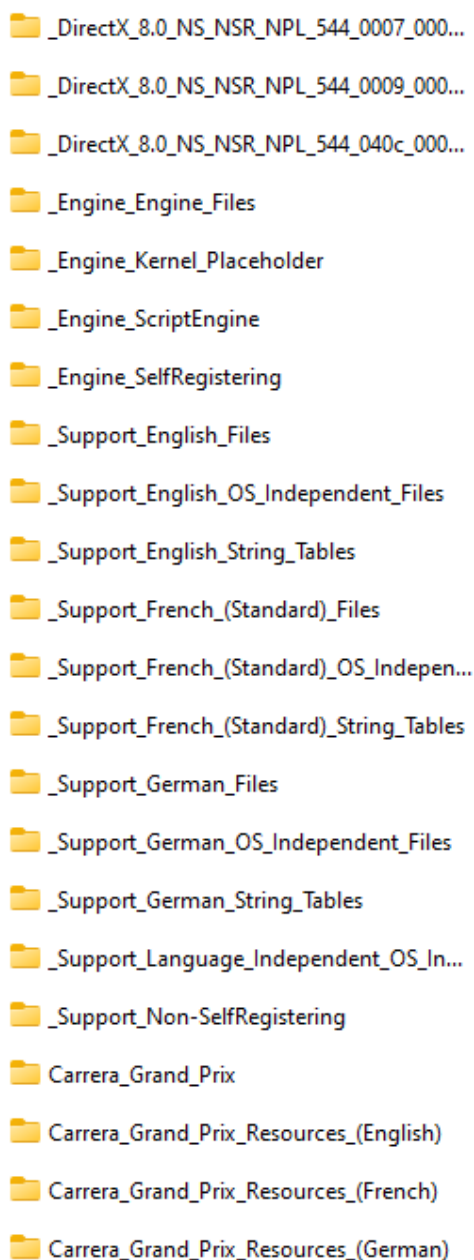
METODO B:

Con il metodo A abbiamo bypassato phenoProtect modificando lo script di installazione, ma esiste anche una seconda possibilità: estrarre tutti i file del gioco senza usare il programma di installazione!

Possiamo usare UniExtract v2 per scompattare gli archivi CAB presenti nel disco del gioco ed ottenere i file. Apriamo UniExtract e scegliamo il file data1.cab:



Non è necessario estrarre anche il file data2.cab in quanto verrà processato automaticamente da UniExtract. Una volta conclusa l'estrazione possiamo spostarci nella cartella di destinazione. Troveremo la seguente lista:



Copiamo la cartella “Carrera_Grand_Prix”, che è quella che contiene i file principali, sul desktop e copiamo al suo interno il contenuto della cartella “Carrera_Grand_Prix_Resources_(English)” (ovvero i file ART0001.RFD ed ART0001.RFH). Ricordate che, se state usando una versione recente di Windows, dovete copiare anche la libreria d3drm.dll scaricata in precedenza e di configurare DxWnd sull’eseguibile _crrr.exe per evitare problemi di compatibilità.

A questo punto possiamo lanciare Carrera.exe e noteremo che invece del tasto con scritto “Play” ne troveremo uno con scritto “Install”. Questo è dovuto al fatto che il gioco non trovando le relative chiavi inserite nel registro di sistema in fase di installazione, crede di dover essere ancora installato.

Possiamo procedere in due modi:

- Usando x32dbg, settando un breakpoint su RegCloseKey e forzando il salto condizionale al ritorno sul codice dell'applicazione
- Installando il gioco con il Metodo A ed effettuando un dump delle chiavi necessarie dal registro

Entrambi i metodi sono efficaci, ma se scegliete il primo, dovrete anche applicare qualche patch in più per disattivare il controllo del disco e reindirizzare la l'apertura del file resource.cfg dal CD alla cartella di installazione del gioco (indirizzo 00403EBB). Inoltre, va anche forzato il salto condizionale presente all'indirizzo 00403B7F per fare leggere al gioco i file dalla cartella corrente.

Se volete usare il secondo metodo, vi basterà installare il gioco ed effettuare, usando regedit, un semplice dump di:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Take2\Carrera Grand Prix

Adesso potete procedere disinstallando il gioco. Modificate dal file .reg (aprendolo con blocco note) il valore della chiave "Path" inserendo il percorso della cartella dove avete estratto i file del gioco ed infine importatelo sul vostro registro. Avviate nuovamente Carrera.exe dalla vostra cartella e funzionerà tutto correttamente. Anche in questo caso, se volete, potete rimuovere il controllo sulla presenza del disco come descritto in precedenza.

Credits:

Ringrazio sentitamente Codecult/Phenomedia AG per aver create questa protezione unica nel suo genere ed interessante.

Ringrazio anche gli autori degli strumenti usati per effettuare questa analisi e realizzare questo documento tecnico.

Conclusione:

È stata una protezione molto divertente da analizzare in quanto totalmente diversa da quelle che ho documentato sino adesso. La sua semplicità, inoltre, la rende perfetta che i principianti e i reverser alle prime armi. Peccato che sia stata usata soltanto in un paio di giochi.

Grazie per la lettura!

Luca