

Modifying Gameshield Licenses – Nieylana

February 2011

Introduction

This tutorial is designed to accompany the unpacking tutorial presented by SSIEvIN, it does not continue on with what he taught in his tutorial but rather we will take a different approach to GameShield. As with most things there is more than one way to get something done, unpacking is surely the best option but for targets that do not want to cooperate perhaps the next best option is to attempt to modify the license files.

In this tutorial we will cover what is needed to properly modify a license file. With the license files open to the world we can manipulate it as we see fit (extend trial period, trial reset, etc). The implications of what is to be detailed here has not been fully explored and it is the wish of the author that you take this information and play around with other applications to see what you can do as far as license modifications go. Some of the basic mods will be detailed here in the course of our learning but it is by no means an exhaustive list.

Because this tutorial has a lot of information to cover in a short time, some things may not be explained to the fullest extent possible, the author assumes that you have a fairly decent grasp on reverse engineering, basic knowledge of cryptography (Blowfish) and the use of common reversing tools such as LordPE.

The information contained in this tutorial is meant for academic purposes only, and is not the work of any one individual. Many have helped with the information provided within the next pages (and tools). Without them and their desire for helping others neither this paper nor the tools provided would have come into being.

The tools provided within this package are provided solely to demonstrate that the techniques we've learned do in fact work. They are not given out so that users may cheat well deserving authors out of money that they're due. If you like an application/game that is protected with GS, BUY IT! Enough of that stuff, let's have some phun!

--Nieylana

Modifying Gameshield Licenses – Nieylana

Disclaimers

All code included with this tutorial is free to use and modify; we only ask that you mention where you found it. This tutorial is also free to distribute in its current unaltered form, with all the included supplements. All the commercial programs used within this document have been used only for the purpose of demonstrating the theories and methods described. No distribution of patched applications has been done under any media or host. The applications used were most of the times already been patched, and cracked versions were available since a lot of time. ARTeam or the authors of the paper cannot be considered responsible for damages to the companies holding rights on those programs. The scope of this tutorial as well as any other ARTeam tutorial is of sharing knowledge and teaching how to patch applications, how to bypass protections and generally speaking how to improve the RCE art. We are not releasing any cracked application.

Verification

ARTeam.esfv can be opened in the ARTeamESFVChecker to verify all files have been released by ARTeam and are unaltered. The ARTeamESFVChecker can be obtained in the release section of the ARTeam site:

<http://releases.accessroot.com>

Table of Contents

1. Modifying GameShield Licenses
 - 1.1. Abstract
 - 1.2. Targets
 - 1.3. Tools Used
2. Reversing the Shell
 - 2.1. Finding/Dumping Protection DLL
 - 2.2. Analyzing DLL
 - 2.3. Recap Attack Method
3. Intercepting Information
 - 3.1. Find License File Password
 - 3.2. Investigating Blowfish
 - 3.3. Decrypt Key Problem (and solution)
4. License Modification
 - 4.1. Decrypt License Data
 - 4.2. Making Changes
 - 4.3. Repacking License
5. Final Thoughts
6. Greetings

Modifying Gameshield Licenses – Nieylana

1. Modifying GameShield Licenses

1.1 Abstract

This tutorial will cover the process of modifying a GameShield (from here on referred to as GS) protected application's license file. In order to do so we must reverse the GS protector to find potential starting points for our attack. Once attack points have been located we must successfully attack the target to recover the required information for the decryption/encryption of the license files. After decrypting the files we must learn the license file format and figure out useful modifications for the files.

Also covered in this tutorial will be how to 'trial reset' an application that's is protected with GS, the ability to trial reset is important for those applications whose license files have become corrupted and for those applications that refuse to unpack via SSIEvIN's unpack method.

1.2 Targets

In order to prevent lengthy downloads I've protected a copy of ARTeam's Xilisoft Crypter tool and set it as a 30-minute demo. It can be found in this tutorial package under the folder 'target'.

This application will be the main focus for the duration of the tutorial, but things learned in this tutorial can easily be used on other 'real' targets if you so choose.

1.3 Tools Used

- Olly debugger v1.10 (um... what's this for again)
 - <http://diablo2oo2.di.funpic.de/downloads/d2k2.ollydbg.public.rar>
- Lord PE (for dumping things)
 - http://www.woodmann.com/collaborative/tools/images/Bin_LordPE_2010-6-29_3.9_LordPE_1.41_Deluxe_b.zip
- DCPCrypt Library (for analysis of their Algorithms)
 - <http://www.cityinthesky.co.uk/files/dpcrypt2.zip>
- Some brain as usual ... (this is NOT optional)
 - No download available
- Maybe some things I forgot to put here lol

Modifying Gameshield Licenses – Nieylana

2. Reversing The Shell

As with any protection system, one important step is to reverse the shell to the extent that we need to be able to successfully attack their system. In our case we are interested in the license files of GS.

2.1 Finding/Dumping Protector DLL

Much like Armadillo for those familiar with it, GS embeds a protector dll in the executable file that is unpacked into memory at runtime. This dll (as we'll see) handles most if not all of their protection logic. Before we can do anything, we first need to find this DLL and dump it to disk to better analyze things

First thing to do is fix the PAGE_NO_ACCESS as mentioned in SSIEvIN's tutorial, but this time we're going to keep our breakpoint on VirtualProtect and continue until we see this in the stack:

```
0092992E CALL to VirtualProtect from Crypter.00929929
00406000 Address = Crypter.00406000
00000400 Size = 400 (1024.)
00000002 NewProtect = PAGE_READONLY
0012FCE4 OldProtect = 0012FCE4
```

Once this is found press Alt+F9 to return to user code, we are now in the DLL unpacking routine. I've taken a snapshot of the code and commented where necessary:

```
0092992E 8BC6 MOV EAX,ESI
00929930 E8 BFFBFFFF CALL 009294F4
00929935 8BF8 MOV EDI,EAX
00929937 4F DEC EDI
00929938 85FF TEST EDI,EDI
0092993A 7C 71 JNC SHORT 009299AD
0092993C 47 INC EDI
0092993D C745 EC 00000000 MOV DWORD PTR [EBP-14],0
00929944 8B55 EC MOV EDX,DWORD PTR [EBP-14]
00929947 8BC6 MOV EAX,ESI
00929949 E8 62F5FFFF CALL 00928EB0 get next Section name
0092994E 8B08 MOV EBX,EAX
00929950 837B 10 00 CMP DWORD PTR [EBX+10],0
00929954 7E 43 JBE SHORT 00929959 skip if NULL section
00929956 8B43 14 MOV EAX,DWORD PTR [EBX+14]
00929959 33D2 XOR EDX,EDX
0092995B 0346 08 ADD EAX,DWORD PTR [ESI+8]
0092995E 1356 0C ADC EDX,DWORD PTR [ESI+C]
00929961 52 PUSH EDX
00929962 50 PUSH EAX
00929963 8B45 E4 MOV EAX,DWORD PTR [EBP-1C]
00929966 E8 B92AFFFF CALL 0091C424
0092996B 8B55 FC MOV EDX,DWORD PTR [EBP-4]
0092996E 0353 0C ADD EDX,DWORD PTR [EBX+C]
00929971 8B4B 10 MOV ECX,DWORD PTR [EBX+10]
00929974 8B45 E4 MOV EAX,DWORD PTR [EBP-1C]
00929977 E8 B42CFFFF CALL 0091C638 unpack section
0092997C 8B43 10 MOV EAX,DWORD PTR [EBX+10]
0092997F 8B53 08 MOV EDX,DWORD PTR [EBX+8]
00929982 3BC2 CMP EAX,EDX
00929984 73 21 JNB SHORT 009299A7 go to loop
00929986 8B4D FC MOV ECX,DWORD PTR [EBP-4]
00929989 034B 0C ADD ECX,DWORD PTR [EBX+C]
0092998C 03C8 ADD ECX,EAX
0092998E 51 PUSH ECX
00929991 2B00 SUB EDX,EAX
00929994 58 POP EAX
00929997 E8 0D02FEFF CALL 00909BA4
00929999 EB 0E MOV EBX,00909BA7
0092999C 8B45 FC MOV EAX,DWORD PTR [EBP-4]
0092999F 034B 0C ADD EAX,DWORD PTR [EBX+C]
009299A2 8B53 08 MOV EDX,DWORD PTR [EBX+8]
009299A7 E8 FD01FEFF CALL 00909BA4
009299AA FF45 EC INC DWORD PTR [EBP-14]
009299AB 4F DEC EDI
009299AB 75 97 JNC SHORT 00929944 increment
decrease section count
unpack next section
```