2012

Keygenning GameShield/SoftwareShield

Nieylana

ARTeam

April 2012

1 DISCLAIMER

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 tutorial 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 by other fellows, and cracked versions were available since a lot of time. ARTeam or the authors of the papers shouldn't be considered responsible for damages to the companies holding rights on those programs. The scope of this document 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.

2 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

ARTEAM QUALITY
100%
GUARANTEED

3 TABLE OF CONTENTS

1 DISCLAIMER 2

2 VERIFICATION 3

3 TABLE OF CONTENTS 4

4 INTRODUCTION 6

5 REQUIREMENTS 7

5.1 Target 7

5.2 Tools 7

6 RESEARCHING THE LICENSE SCHEME 8

6.1 Authorization Definitions (AD) 8

6.2 Authorizations Request Codes (ARC) 8

6.3 Activation codes (AC) 9

6.4 Serial Numbers 9

7 RETRIEVING THE GLOBAL AND LICENSE PASSWORDS 10

7.1 Dumping the DLL 10
7.1.1 Bypassing The Stack Overflow 10
7.1.2 Locating Unpack Routine 11
7.1.3 Getting the DLL 12

7.2 Checking the Exports 13

7.3 Getting function signatures 15

7.4 Writing the password stealer 15
7.4.1 Outlining requirements 16
7.4.2 Starting the process 16
7.4.3 Fixing Virtual Protect PAGE_NOACCESS 16
7.4.4 Watching for the Functions to unpack 17
7.4.5 Waiting for the breakpoints to hit 18
7.4.6 Cleaning up and closing down 18
7.4.7 Output for GameShield 4.6 19

8 GETTING THE AUTH PASSWORD 20

8.1 Decrypting The License 20

8.2 License File Format 21

8.3 Using the Delphi Parser 23

8.4 Choosing an Authorization Definition 24

9 BUILDING A KEY 26

9.1 Decrypting an ARC 26

9.2 Making an Activation Code 28

10 CONCLUSION 31

4 INTRODUCTION

About 1 year ago I released a paper discussing how to modify GameShield/SoftwareShield licenses. While it was an interesting adventure and the limit to the possibilities of the attack remain unknown perhaps it was not the most viable solution to the protector. While the attack showed some vulnerabilities in the protector it did not fully compromise GameShield since it wasn't easily distributable through the 'scene'. I have hesitated to discuss Keygenning since it would allow piracy of the games/apps protected with the software, however it is NOT the ARTeam spirit to withhold information from the community. Information is held only long enough to responsibly release it to the world.

So why release the information now if it will enable piracy? Isn't ARTeam against piracy??? Yes, we do not support it, however there are very few targets that this fully compromises, 99% of games/applications use a server check of some sort, so while we can make valid keys software cannot be activated with them due to the server checks. While solutions exist to the server check, this will NOT be discussed in the paper. There is however One application that allows for offline activation :) This is the target we will be discussing.

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), the use of common reversing tools such as LordPE, and programming knowledge (examples are in C#). The author assumes that you have read the previous tutorial(s) on GameShield and have some familiarity with its internals (handling of crypto specifically).

The goal of this tutorial is to show what GameShield/SoftwareShield does and how to mimic their processes to yield valid keys, unfortunately due to the scope of the topic a step-by-step explanation of how things were discovered is not practical. I will do my best to give the proper amount of details so that one can fully understand what’s going on.

The information contained in this tutorial is meant for academic purposes only, and is only demonstrated to point out flaws in the protector. Many have helped with the information provided within the next pages (and tools). Without them and their desire for helping others neither this paper couldn't have been written.

Any tools/sources 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!