SSLEVIN [ARTEAM]

Manual unpacking of Gameshield v4.5

February 2011

1. Introduction

GameShield protector is relatively unknown to the RE scene. Current version is at 4.5. If you look their homepage here: http://www.gameshield.com/Overview/Benefits.aspx you will see that it really offers a lot of protection options for companies that create and distribute PC video games.

OK, then, how come that such good game protector remained in a relatively “safe haven” and untouched by reversers always hungry for new challenges ? (SIDENOTE: Even famous all round tool for detecting protection used on .exe/.dll, Protection ID does not detect it as Gameshield, but as “Possible CD/DVD-Key or Serial Check -> ActivationCode”. Well, actually its true, but does not help much really.)

Well, I could point out that lack of interest for this protector comes out of the fact that most game titles at Namco games (http://www.namcogames.com) and Legacy games (http://www.legacygames.com) can be obtained at other game portals which use more familiar protectors like Armadillo, ActiveMark etc. etc.

On the other hand developers are kinda lazy or they are not aware of all protective capabilities of GameShield. In my investigating process I tried reversing maybe a dozen of GameShield protected targets and only a few of them used multiple file protection or com based protection which makes unpacking a real pain in the arse. Most of the targets (Try/Buy, as well as Buy Only) use just basic type of protection (Nag Screen with option to enter Serial Number or Activation Code) which makes them (as you will see in this paper) an easy prey.

When you first try to reverse this, it really looks as terrifying tiger, but by the end of this document you will realize it is actually a purring cat in your hands.

Happy reversing,

SSlEvIN.

Manual unpacking of Gameshield v4.5

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

Manual unpacking of Gameshield v4.5

1. Manual unpacking of GameShield v4.5

1.1. Abstract

In this tutorial will be shown the basic unpacking approach (reaching targets OEP), dumping target from memory and fixing imports. Possible troubles in that you can fall during unpacking will also be shown as far as author knows about them. In the end, how to play Gameshield protected Buy Only targets “for this execution only” will also be shown.

1.2. *Targets*

StarDefender4(Try&Buy):
http://www.namcogames.com/pc_games/star_defender4
Direct download link(11,56MB):
http://c0157431.cdn.cloudfiles.rackspacecloud.com/portal/StarDefender4.exe

MementoMori(BuyOnly):
http://www.legacygames.com/download_games/1369/memento_mori
Direct download link (2.14GB):
http://legacygames.com/downloads/MementoMori-Setup.exe

NOTE: Try reversing these two on your own after reading the tutorial:
(Burger Time Deluxe (Try&Buy):
http://www.namcogames.com/pc_games/burgertime_deluxe
Direct download link (40,63MB):
http://c0157431.cdn.cloudfiles.rackspacecloud.com/BurgerTime_Deluxe_101112.exe

Mishap 2: An Intentional Haunting(Try&Buy):
http://www.namcogames.com/pc_games/mishap2
Direct download link (643MB):
http://c0157431.cdn.cloudfiles.rackspacecloud.com/Mishap2_CE_w2.exe)

NOTE: I am really sorry for the download size of some targets, but I really hope you will manage to get them and try the things described in lines that follow.

1.3. Tools used

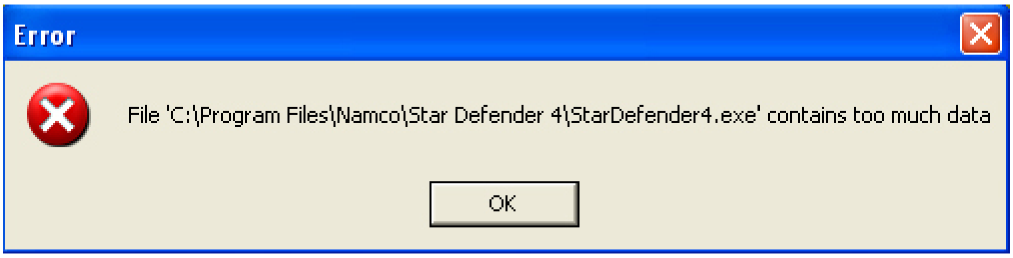
- Protection ID v6.4.0
- Olly debugger v1.10
- Lord PE
- ImPREC
- WinHex or any other hex editor that can open memory of a running process
- CFF Explorer
- ResHacker
- Some brain as usual …

2. General unpacking approach for all Gameshield targets

2.1. At first glance (nothing important, but nice to know)

Prior to opening your target in Olly, it is highly recommended to scan it with Protection ID and also to scan all the files inside target directory. Protection ID, as I already said, won't tell you the name of the protector but you will find out many usefull things, i.e. are there other files inside target directory that are protected or is your target using overlay (Youda Safari, for example). Appending overlay to the EOF does not differ from any other protector, thus I did not choose this target for tutorial.

After scanning, open your target in Olly. Lets start with StarDefender4. As soon as you open it your devoted debugger shoot this message:



File 'C:\Program Files\Namco\Star Defender 4\StarDefender4.exe' contains too much data

FIGURE 1. Error message

Well, nothing to worry about really. If this message is annoying for you, you can easily fix it, but it does not affect the process of unpacking by any mean. It is just protectors attempt to hide file sections from the reversers keen eye. Press OK and Olly will stop at protectors entrypoint. Press Alt+M and above message should be more clear to you. Where are file sections ? You see only this: