2008

Generating Keys for TimePassages

Author: Nacho-Dj

Graphic Editor: Shub-Nigurrath

ARTeam

July 2008

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.

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

TABLE OF CONTENTS

1 FOREWORDS

In this document a deep analysis for getting valid keys to register the TimePassages commercial software is done.

The main feature which turned this application attractive is the protection used by the software. It follows a method that involves some encryption.

Another issue to get it more attractive is the no existence of any Key Generator for this target.

Patching some areas of the code gives the appearance to get it registered, but a further analysis reveals that is just an illusion, due to the existing encryption code.

Thus, we are facing a good protection, and by analyzing it you could get a new point of view about the way of reversing some kind of targets using similar methods.

Happy entertainment.

Nacho_dj

ABSTRACT

In this tutorial we are going to analyze a target protected by a strong method, and after that, we could deduce all of the necessary to build a Key Generator (keygen) and get registered with valid keys.

The way of finding any working key to get registered could be more or less difficult, as it happens in any other protected software, but there is a limitation: if we are not correctly registered, we cannot access some content of files used by the target. Which could be the reason?

Well, these files have been encrypted; in that way is useless trying to access their content. Only strange symbols could be seen, in appearance arbitrary ones of the binary values composing the content of the file. After using a valid key to register, we will be able to extract the content of any file as text by using the software.

Thus, we know something in advance: a good key activates, in some way, the decryption process for the protected files.

Let's start to face it...

1.1 TARGET

In this case, it is a neither protected nor packed executable, so it can be debugged without any problem.

Here is the link to the product site:

http://www.astrograph.com/downloads/

Here is the link to download the target:

http://www.astrograph.com/downloads/Win50Base.exe