2009

Serial Fishing and Creating a Self Registering Program

R@dier

ARTeam

June 2009

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

TABLE OF CONTENTS

1 APPROACHING THE PROBLEM

INTRODUCTION

I noticed that the approach to make a target program self registering has not been discussed for quite some time so I am adding this tutorial to the ARTeam beginner olly tutes

What you will need for this tutorial is:

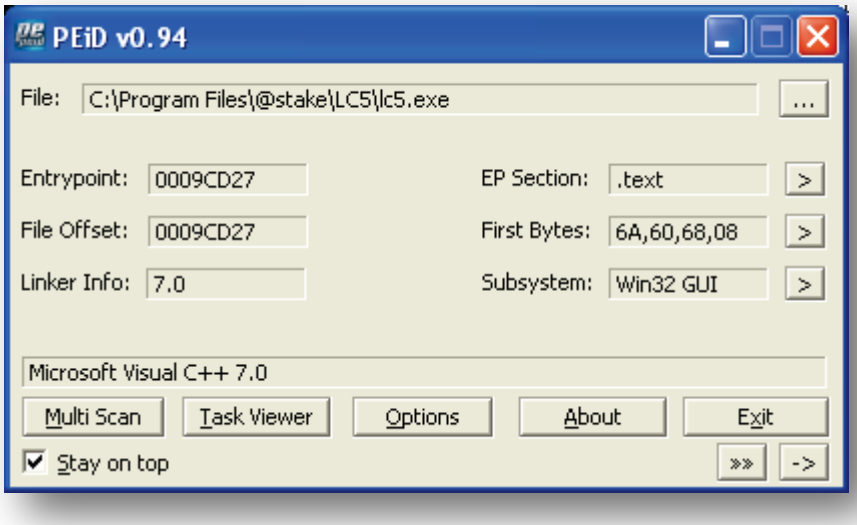
1. OllyDbg 1.10
2. PeID
3. Some assembly knowledge

Today's target for this demo is LC5 a Password and Auditing tools.

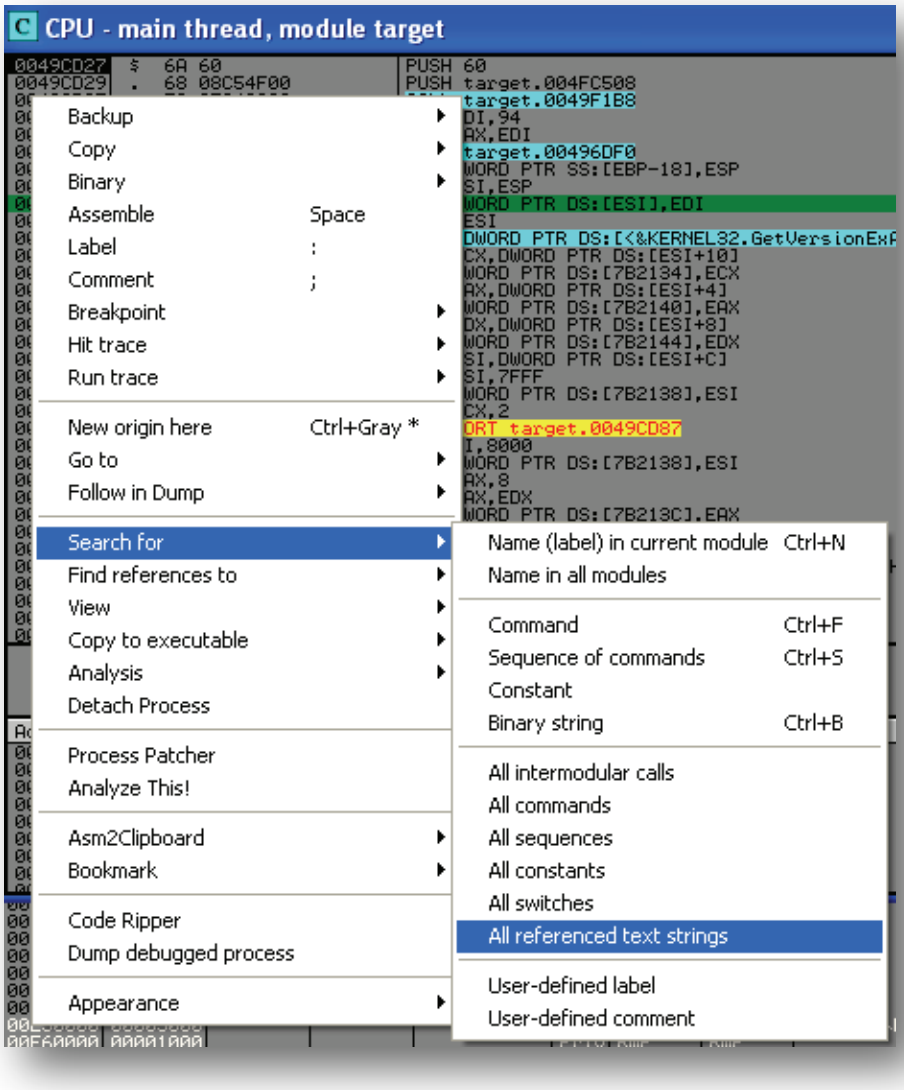
STARTING THE HOMEWORK

Ok let's get started

Startup PeID and check the program for any protector's/ packers, as we can see the program is clear of any protections so let's get started



Open up the target program in ollyDbg and you should land here, the first thing we are going to do is check for any text string that can give us a starting point in the application. To do this right click the screen and go to Search for → All referenced text Strings

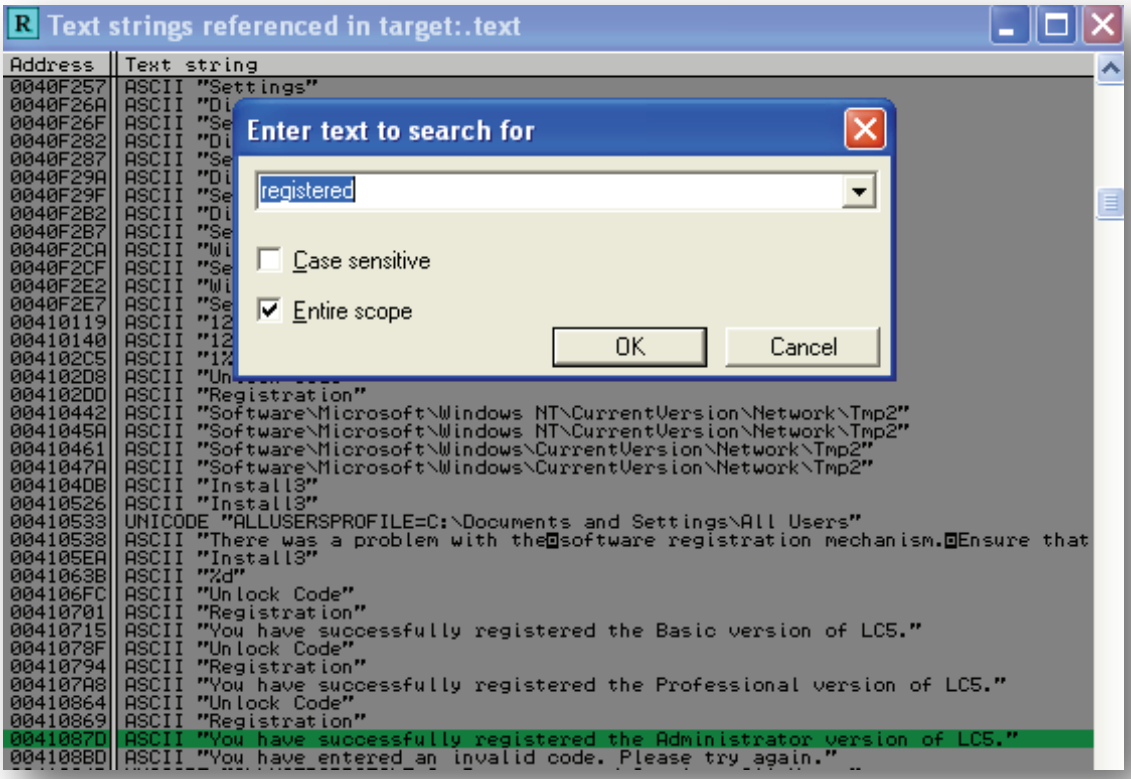


Once in the code window, do a CRTL + L to bring up the search window, type in **registered** then press ok

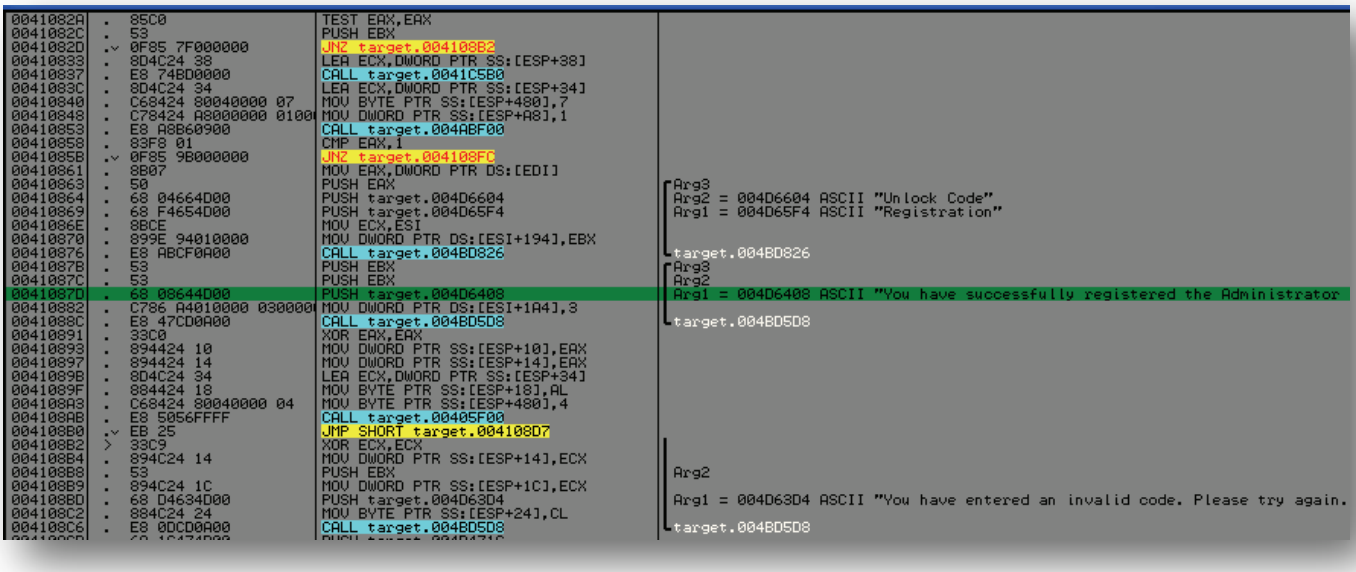
You should end up around here. To keep searching for the next instance of the search word you can keep pressing **CRTL + L**

If you look down at the highlighted line you can see there are three types of registrations available, Basic, Professional and Administrator.

We are interested in the best option so double click on the **"You have successfully registered the administrator version of LC5"**



You will land here:



From the code above we can see there are two cases that can occur,

a successful registration or an **"You have entered and invalid code"** message.