DEROKO OF ARTEAM

Dealing with funny checksum

Version 1.0
February 2013

1. Forewords

After a while, I've decided to write about something interesting which I've found while unpacking one protection, and it will be also nice introduction to one of my tools which I have wrote for fun of it.

However, I won't mention application name here, but to demonstrate checksum check which I have found I will be using one test application, thus you will get idea what happened, and how checksum is defeated

I will also introduce one tool I wrote, which served me well in this particular case. Tool should come with this document, thus I won't describe tool, and it's internals as source code should be well commented

deroko of ARTeam

Editor: deroko

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 damages 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