2009

ARTeam eZine Issue IV

Editor: Shub-Nigurrath

ARTeam

3/25/2009

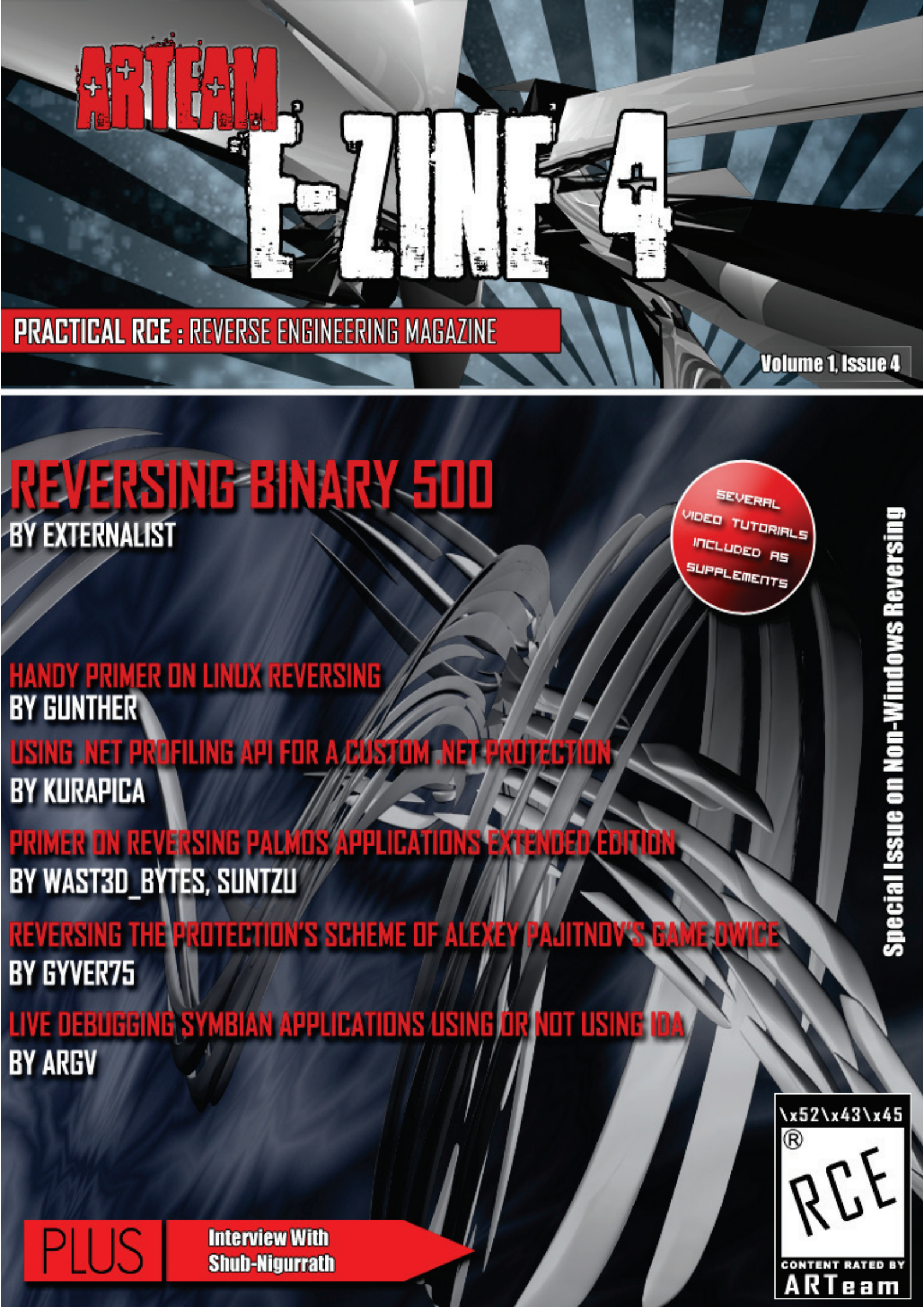
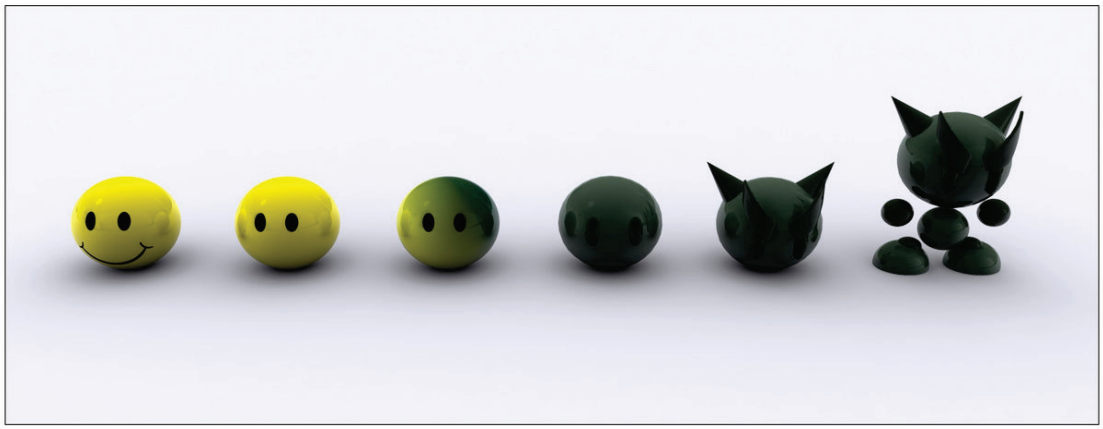

ARTEAM
E-ZINE 4
PRACTICAL RCE : REVERSE ENGINEERING MAGAZINE
Volume 1, Issue 4
REVERSING BINARY 500
BY EXTERNALIST
SEVERAL VIDEO TUTORIALS INCLUDED AS SUPPLEMENTS
HANDY PRIMER ON LINUX REVERSING
BY GUNTHER
USING .NET PROFILING API FOR A CUSTOM .NET PROTECTION
BY KURAPICA
PRIMER ON REVERSING PALMOS APPLICATIONS EXTENDED EDITION
BY WAST3D_BYTES, SUNTZU
REVERSING THE PROTECTION'S SCHEME OF ALEXEY PAJITNOV'S GAME DWICE
BY GYVER75
LIVE DEBUGGING SYMBIAN APPLICATIONS USING OR NOT USING IDA
BY ARGV
Special Issue on Non-Windows Reversing
PLUS
Interview With Shub-Nigurrath
\x52\x43\x45
RCE
CONTENT RATED BY ARTeam

TABLE OF CONTENTS

FOREWORDS



. E V O L U T I O N .

Hi all,

It's a long time since I promised the new ARTeam issue. As usual I had to postpone this new issue for a long time due to a lot of things happened in the meantime. As anyone following us probably knows we had to change hosting, rebuild the database of the forums and re-create the web site. All those stuffs have not been a snap and I must excuse with authors who sent to me their contributions some months ago. Anyway we are back now and hopefully we are here to stay. **Now we are hosted at www.accessroot.com write it down!**

This issue is then dedicated to the ·EVOLUTION·. Evolution ... means a lot of things indeed..

First of all, evolution of the reverse engineering world, this is evolving under the pressure of different issues. One is the appearance of new post-pc devices and the increasing interest in reversing non Windows worlds, the second is the augmented number of professionals involved in this area, on both sides of the barricades. The result is that the reversing skills required to stay at the edge are increasing each and every day. It's not as simple to be original and to release new things, to follow all the possible directions. To stay on top requires constant study and updating and this can be done only in two situations: when you are a kid without a work, or a student, when you are paid by someone (either from black or white reversing worlds). Moreover the economical crisis affecting most parts of the world is not helping! So what to happen? As with all things, we also have to evolve somehow...

The scene is rapidly changing; everyone would really have to agree that cracking is slowly fading away, but not away to oblivion, away to something else. The amount of protections or cool ideas is becoming less frequent, yet on the other hand the protections are becoming more and more complex.

A few years ago, the software industry created new official competences: the Secure Software Development Lifecycle developer, the Security Architect and the Professional Reverse Engineer. This was due to the fact that finally reversing for security needs was recognized as a necessity and has been regulated by laws (since year

The reverse engineering world, is evolving under the pressure of different issues. One is the appearance of new post-pc devices, the second is the augmented number of professionals involved in this area, on both sides of the barricades

2000), so it's now possible to build a career based solely upon reversing. This was not possible at the times of +Fravia or +HCU, so the industry suffered with a lack of professionals figures for reversing/protecting applications. The effect of this change of scenario is under everyone eyes: a big and constant rising of the bar under economic pressure. New protections (Themida, SecuROM,...) and malware witness a change of attitude (you may think that they are complex or not, but they are surely a breaking evolution compared to older things). How many crackers can handle them fully? Not many and those who are keep their secrets for their own clubs.

Which is the solution, I am not sure. I do know what it should be: share and work together, adopting the same methods used by the "official" scientific reversing community. I'll call it scientific reversing, it publishes papers, ezines, forums, conferences... but most of all collaboration is the keyword!

Collaboration is the keyword: software and protection industry collaborates; malware industry collaborates (on both sides). A friend wrote little time ago "*reversers should be more of a team, rather than acting like a loosely knitted group of individuals. That is not to say that we shouldn't have our own individual projects/desires, but there isn't really a sense of direction or purpose, other than to share what we find on our journeys... Sometimes we are blindsided by our own singlemindedness, and fail to see new opportunities that are there...At the same time as achieving this, you then get an improvement in everybodies skills and knowledge, because ALL get taken along together.*" Ask yourself, what made +HCU what it was? I think that were two things: a truly sense of wonder and a team thinking (all together aiming at a final result).

For these reasons I want to raise my hand and call for quality contributors and reversers willing to share original new tutorials and experiences. Sharing for what? To keep this experience alive. ARTeam is not our child, is an instrument you may use or not.

So if you want to contribute with tutorials about reversing *anything* or describing original attacks and advanced approaches you are invited to contact us/me.

Coming to this issue, **it is focused on non-windows reversing, or better on non-win32 reversing**. There are insights into the Linux world (Externalist, Gunther) and the Palm (wast3d_bytes has released independently another Palm issue, which has been extended exclusively for this eZine, I also added an interesting video tutorial from Suntzu). There are also two interesting contributions into .NET advanced concepts and one about classical reversing from Gyver75, which I added for the passion for reversing it clearly shows, besides quality of the work. This walkthrough is completed by a series of video tutorials prepared by argv about live debugging Symbian systems, not only using IDA. The non-win32 tutorials are just a completion of the activity we had already started a long time ago, investigating new reversing worlds like the already known Symbian, iPhone, .NET and Mac. Finally, I decided to add an interview Gunther prepared for me. It was requested a long time ago, you may skip it ;-)

Anyway as you can see the result is another extremely long issue, probably the longest one till now. All the times it happens to write such a big issue I ask myself: how many of you will read or appreciate it, how many will appreciate these "forewords" –hehe-. I really don't know. **One thing I must say is that each chapter can be printed separately, which is especially true for this issue, because each one belongs to completely different worlds.**

Your Favourite Neighbourhood Shubby

DISCLAIMER/LICENSE

All code included with this tutorial is free to use and modify; we only ask that you mention where you found it. This eZine is also free to distribute in its current unaltered form, with all the included supplements.

We have potentially illegal stuff inside. All the commercial programs used within our tutorials have been used only for the purpose of demonstrating the theories and methods described. These documents are released under the license of not using the information inside them to attack systems of programs for piracy. If you do it will be against our rules. 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. We are not at all encouraging people to release cracked applications; damages if there will be any have to be claimed to persons badly using information, not under our license.

This disclaimer applies to all ARTeam releases and tutorials!

SUPPLEMENTS

This eZine is distributed with Supplements for each paper; the supplements are stored in folders with the same title of the paper. Almost all the papers have supplements, check it.

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