



Windows Malware Analysis **Accelerated**

with Memory Dumps

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2013 by OpenTask

Copyright © 2013 by Memory Dump Analysis Services

Copyright © 2013 by Dmitry Vostokov

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of the publisher.

You must not circulate this book in any other binding or cover and you must impose the same condition on any acquirer.

Product and company names mentioned in this book may be trademarks of their owners.

OpenTask books and magazines are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

A CIP catalogue record for this book is available from the British Library.

ISBN-13: 978-1-908043-44-3 (Paperback)

First printing, 2013

Contents

Introduction.....	5
Practice Exercises	15
Exercise 0: Download, setup and verify your WinDbg installation	20
Exercise M1A	30
Exercise M1B	43
Exercise M2	55
Exercise M3	73
Exercise M4	124
Exercise M5	182
Exercise M6	210