



# Windows Malware Analysis **Accelerated** **with Memory Dumps**

**Version 2.0**

Dmitry Vostokov  
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2017 by OpenTask

Copyright © 2017 by Software Diagnostics Services

Copyright © 2017 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](mailto:press@opentask.com).

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

ISBN-13: 978-1-908043-86-3 (Paperback)

Revision 2.02 (October 2017)

# Contents

About the Author.....	5
Introduction.....	7
Practice Exercises .....	17
Exercise 0: Download, setup and verify your WinDbg installation .....	22
Exercise M1A .....	35
Exercise M1B .....	48
Exercise M2.....	60
Exercise M3.....	77
Exercise M4.....	130
Exercise M5.....	186
Exercise M6.....	210
Selected Q&A.....	232
Appendix.....	235
Malware Analysis Patterns .....	237
Deviant Module .....	237
Deviant Token.....	244
Driver Device Collection .....	245
Execution Residue .....	246
Fake Module .....	270
Hidden Module.....	274
Hidden Process .....	276
Hooksware.....	278
Namespace .....	279
No Component Symbols.....	280
Out-of-Module Pointer.....	283
Packed Code .....	284
Patched Code.....	287
Pre-Obfuscation Residue .....	288
Raw Pointer .....	289
RIP Stack Trace .....	290
Self-Diagnosis (Kernel Mode) .....	292
Stack Trace Collection .....	293
Stack Trace Collection (I/O Requests) .....	301

String Hint.....	305
Unknown Module.....	307
Raw Stack Dump of All Threads (Kernel Space).....	310
Complete Stack Traces from x64 System .....	311