



Defect

→  
Detect

# Windows Malware Analysis **Accelerated**

**with Memory Dumps**

**Version 3.0**

Dmitry Vostokov  
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2022 by OpenTask

Copyright © 2022 by Software Diagnostics Services

Copyright © 2022 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 publisher's prior written permission.

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: 978-1-912636-96-9 (Paperback)

Revision 3.00 (July 2022)

# Contents

About the Author.....	5
Introduction.....	7
Practice Exercises .....	17
Exercise 0: Download, setup, and verify your WinDbg Preview or WinDbg installation, or Docker Debugging Tools for Windows image.....	22
Exercise M1A .....	38
Exercise M1B .....	49
Exercise M2.....	64
Exercise M3.....	81
Exercise M4.....	133
Exercise M5.....	187
Exercise M6.....	211
Selected Q&A.....	243
Appendix.....	247
Malware Analysis Patterns .....	249
Deviant Module.....	249
Deviant Token.....	256
Driver Device Collection .....	257
Execution Residue .....	258
Fake Module.....	282
Hidden Module.....	286
Hidden Process .....	288
Hooksware.....	290
Namespace .....	291
No Component Symbols.....	292
Out-of-Module Pointer.....	295
Packed Code .....	296
Patched Code.....	299
Pre-Obfuscation Residue.....	300
Raw Pointer .....	301
RIP Stack Trace .....	302
Self-Diagnosis (Kernel Mode) .....	304
Stack Trace Collection .....	305

Stack Trace Collection (I/O Requests) .....	313
String Hint.....	317
Unknown Module.....	319
Raw Stack Dump of All Threads (Kernel Space).....	322
Complete Stack Traces from x64 System .....	323