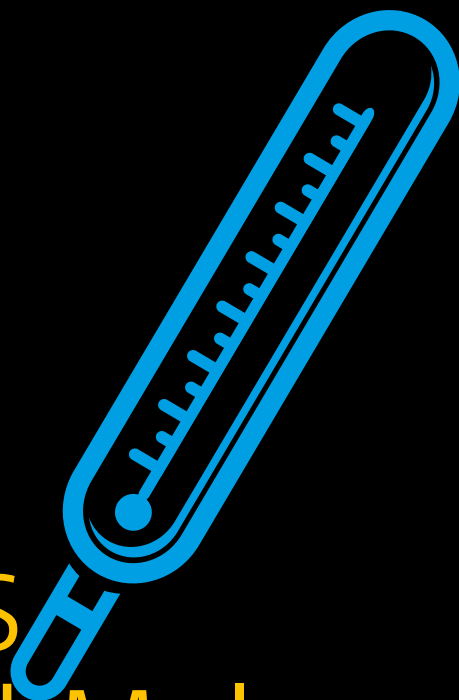


WINDOWS TROUBLESHOOTING SERIES



Windows Virus and Malware Troubleshooting

Andrew Bettany, MVP
Mike Halsey, MVP

Apress®

Windows Troubleshooting Series

Mike Halsey, MVP
Series Editor

Apress®

Windows Virus and Malware Troubleshooting



Andrew Bettany, MVP

Mike Halsey, MVP

Apress®

Windows Virus and Malware Troubleshooting

Andrew Bettany
York, North Yorkshire, United Kingdom

Mike Halsey
Sheffield, South Yorkshire, United Kingdom

ISBN-13 (pbk): 978-1-4842-2606-3
DOI 10.1007/978-1-4842-2607-0

ISBN-13 (electronic): 978-1-4842-2607-0

Library of Congress Control Number: 2017934653

Copyright © 2017 by Andrew Bettany and Mike Halsey

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image, we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr
Editorial Director: Todd Green
Acquisitions Editor: Gwenan Spearing
Development Editor: Laura Berendson
Technical Reviewer: Massimo Nardone
Coordinating Editor: Nancy Chen
Copy Editor: Michael G. Laraque
Compositor: SPi Global
Indexer: SPi Global
Artist: eStudio Calamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484226063. For more detailed information, please visit www.apress.com/source-code/.

Printed on acid-free paper

*Thanks, Mike, for your vision in creating this troubleshooting series.
I hope after reading this book, some readers will be saved
from the pain otherwise incurred by malware. Stay safe.*

—Andrew Bettany

*With many thanks to Grzegorz Tworek and the security researchers at CQure.pl
for providing a test virus, and for their help in making this book possible.*

—Mike Halsey

Contents at a Glance

About the Authors.....	xiii
About the Technical Reviewer	xv
Windows Troubleshooting Series	xvii
■ Chapter 1: What Is Malware?	1
■ Chapter 2: Prevention and Defense	9
■ Chapter 3: Malware Defense in Depth	21
■ Chapter 4: Identifying Attacks.....	41
■ Chapter 5: External Malware and Virus Resources	57
■ Chapter 6: Manually Removing Malware	79
Index.....	93

Contents

About the Authors.....	xiii
About the Technical Reviewer	xv
Windows Troubleshooting Series	xvii
■ Chapter 1: What Is Malware?	1
A Brief History of Malware	1
The Psychology of Infection?	2
Different Types of Malware.....	3
Viruses and Worms.....	4
Spyware.....	4
Adware	4
Trojans	4
Bots	4
Rootkits/Bootkits	5
Backdoors.....	6
Ransomware.....	6
Spam and Phishing E-mails.....	6
The Future of Malware	7
Summary	8
■ Chapter 2: Prevention and Defense	9
Organizational-Level Security	10
Core Microsoft Security Features.....	10
Security Center/Security and Maintenance	11

User Account Control	11
Windows Firewall/Advanced Firewall.....	12
Malicious Software Removal Tool	13
Windows Update.....	13
Windows Startup Security.....	14
BitLocker Encryption	14
Secure Boot	15
Trusted Boot	15
Early Launch Anti-Malware.....	15
Anti-Malware Features.....	16
Windows SmartScreen	16
Windows Defender/Security Essentials.....	17
Windows Defender Offline	17
Other Security Features	18
App Containers	18
32-Bit (x86) and 64-Bit (x64) PCs	19
Restricting Access to Files	19
Summary.....	20
■ Chapter 3: Malware Defense in Depth	21
Firewalls.....	21
Keylogging Software	23
Software Firewalls	24
Organizational Firewalls.....	25
Blacklists and Whitelists	26
The Rise of the Internet of Things.....	27
The Windows Advanced Firewall	27
Demilitarized Zone	32

User Account Control.....	35
Summary.....	39
■ Chapter 4: Identifying Attacks.....	41
How Malware Infects PCs.....	41
Infector-Type Viruses	42
Rootkits and Boot Sector Viruses	44
Macro Viruses	45
E-mail and the Internet.....	46
How Malware Infects Networks	46
Network-Based Security.....	49
Identifying External Attacks.....	50
Firewall Attacks and DDoS	50
E-mail-Borne Viruses and Ransomware	51
Spear Phishing	53
Targeted Application Hacking	53
Identifying Internal Attacks	54
Summary.....	56
■ Chapter 5: External Malware and Virus Resources	57
Malware Protection Center.....	57
Get Updates for Security Software	58
Download Security Software	60
Get Microsoft Support.....	61
Microsoft Baseline Security Analyzer	63
Windows Defender	65
Third-Party Malware and Malware Removal Tools in Depth.....	68
Malicious Software Removal Tool	69
Windows Defender Offline	70

Microsoft Safety Scanner	72
Diagnostics and Recovery Toolset (DaRT).....	73
Windows Defender Advanced Threat Protection	76
Summary	77
■ Chapter 6: Manually Removing Malware	79
Manually Removing Malware	79
Step 1: Isolate the PC.....	79
Step 2: Identify the Running Process(es)	80
Step 3: Deactivate the Malware.....	81
Step 4: Test the Results	84
Step 5: Retest the PC.....	86
Step 6: Remove the Malware.....	86
Rootkit Removal	87
Using BCDEdit	89
Summary	91
Index.....	93

About the Authors



Andrew Bettany has been a Microsoft Most Valuable Professional (MVP) since 2012, in recognition for his Windows expertise.

As a Microsoft Certified Trainer, Andrew provides expertise and consultancy services to businesses in a number of technical areas, including Windows deployment and troubleshooting.

He cofounded and manages the IT Masterclasses series of short technical courses, available at www.itmasterclasses.com, and is passionate about learning and helping others. He is also a frequent speaker at conferences worldwide. In 2011 and 2013, he

delivered a training boot camp in earthquake-hit Haiti to help the community rebuild its technology skills.

Active on social media, Andrew can be found on LinkedIn, Facebook, and Twitter. He lives in a village just outside the beautiful city of York, in Yorkshire, UK.



Mike Halsey was first recognized as a Microsoft MVP in 2011. He is the author of more than a dozen books on Windows, including *Troubleshooting Windows 7: Inside Out*, *Troubleshoot and Optimize Windows 8: Inside Out*, *Beginning Windows 10*, *Windows 10 Troubleshooting* and *The Windows 10 Accessibility Handbook* from Apress. He is also the author of other troubleshooting books related to Windows in this series. Based in Sheffield, UK, where he lives with his rescue border collies, Evan and Robbie, Mike gives many talks on

Windows subjects, from productivity to security, and makes how-to and troubleshooting videos under the banners PCSupport.tv and Windows.do. You can follow him on Facebook and Twitter at @PCSupportTV.