SYNGRESS®

Mobile Malware Attacks and Defense

The Only Book for Analyzing and Mitigating Mobile Malicious Code!

- Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks
- Analyze Mobile Device/Platform Vulnerabilities and Exploits
- Mitigate Current and Future Mobile Malware Threats

Ken Dunham, Technical Editor

Saeed Abu-Nimeh
Michael Becher
Seth Fogie
ian Hernacki
se Andre Morales
aig Wright

Mobile Malware Attacks and Defense

Ken Dunham Technical Editor

Saeed Abu-Nimeh
Michael Becher
Seth Fogie
Brian Hernacki
Jose Andre Morales
Craig Wright

Unique Passcode

28475016

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-298-0

Publisher: Laura Colantoni
Acquisitions Editor: Brian Sawyer
Technical Editor: Ken Dunham
Developmental Editor: Gary Byrne
Cover Designer: Michael Kavish

Page Layout and Art: SPI
Copy Editor: Mike McGee
Indexer: SPI
Project Manager: Andre Cuello

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

Library of Congress Cataloging-in-Publication Data

Dunham, Ken.
Mobile malware attacks and defense / Ken Dunham
p. cm.
ISBN 978-1-59749-298-0
1. Cellular telephone systems--Security measures. 2. Mobile communication systems--Security measures.
3. Mobile computing--Security measures. 4. Computer crimes--Prevention. 5. Computer crimes--Case studies.
6. Computer hackers. 7. Wireless Internet--Security measures. I. Title.
TK5102.85.D86 2008
005.8--dc22

2008042884

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, please visit **www.syngress.com**. Once registered, you can access your e-book with print, copy, and comment features enabled.

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable e-book format. These are available at **www.syngress.com**.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Please contact our corporate sales department at corporatesales@elsevier.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Please contact our corporate sales department at corporatesales@elsevier.com for more information.

Technical Editor

Ken Dunham (CISSP, GSEC, GREM, GCFA, GCIH Gold Honors) has more than a decade of experience on the frontlines of information security. As director of global response for iSIGHT Partners, he oversees all global cyber-threat response operations. He frequently briefs upper levels of federal and private-sector cyber security authorities on emerging threats, and he regularly interfaces with vulnerability and geopolitical experts to assemble comprehensive malicious code intelligence and to inform the media of significant cyber threats. A major media company identified Mr. Dunham as the top quoted global malicious code expert in 2006.

Mr. Dunham regularly discovers new malicious code, has written antivirus software for Macintosh, and has written about malicious code for About.com, SecurityPortal, AtomicTangerine, Ubizen, iDEFENSE, and VeriSign. He is one of the pioneers of Internet community antivirus support with Web sites rated as the best global resource by *Yahoo Internet Life*, *PC Week*, AOL, and many others. Mr. Dunham is a member of the High Technology Crime Investigation Association (HTCIA), Government Emergency Telecommunications and Wireless Priority Service, AVIEN, Virus Bulletin, InfraGard, an RCG Information Security Think Tank, CME, and many other private information-sharing channels. Mr. Dunham also participated in the CIA Silent Horizon (blue team) and DHS CyberStorm (observer) exercises.

Mr. Dunham is a certified reverse engineer and regularly analyzes emergent exploits and malicious code threats and actors targeting client networks. He also works as a Wildlist Reporter each month with the Wildlist organization. He is the author of several books and is a regular columnist for an information security magazine. Mr. Dunham is also the founder of the Boise Idaho Information Systems Security Association (ISSA) and Idaho InfraGard chapters.

Ken wrote Chapters 1, 2, 3 and 6 (the introduction, visual payloads, timeline threats, and vishing).

Contributing Authors

Saeed Abu-Nimeh is a Ph.D. candidate at Southern Methodist University. His research focuses on network and e-mail security. He is interested in studying phishing and pharming attacks and spends his time developing solutions to thwart electronic identity theft and protect mobile users against various types of attacks. He is a member of IEEE, the Anti-Phishing Working Group (APWG), and SMU High Assurance Computing and Networking (HACNet) Lab.

Saeed wrote Chapter 6 (Phishing, Smishing, and Vishing).

Michael Becher received his master's degree in computer science in the year 2006 from RWTH Aachen University of Technology, Germany. He is currently a Ph.D. candidate at the University of Mannheim, Germany, researching on the security of mobile devices like smartphones, sponsored by mobile network operator T-Mobile. One of Michael's main research topics is dynamic analysis of mobile malware and software in general.

Michael worked on several topics in the security area previously, where he authored an article about direct memory access in FireWire and a book about Web application firewalls.

Michael wrote Chapter 8 (Analyzing Mobile Malicious Code).

Seth Fogie is the VP of Dallas-based Airscanner Corporation, where he oversees the development of security software for the Windows Mobile (Pocket PC) platform. He has coauthored numerous technical books on information security, including the best-selling *Maximum Wireless Security* and *Windows Internet Security: Protecting Your Critical Data* from Sams Publishing, *Security Warrior* from O'Reilly, and *Cross Site Scripting Attacks: XSS Exploits and Defense* from Syngress. Seth frequently speaks at IT and security conferences/seminars, including Black Hat, Defcon, CSI, and Dallascon. In addition, Seth has coauthored the HIPAA medical education course

for the Texas Medical Associate and is acting site host for security for InformIT.com, where he writes articles and reviews/manages weekly information security-related books and articles.

Seth wrote Chapter 7 (Operating System and Device Vulnerabilities) and Chapter 10 (Debugging and Disassembly of MM).

Brian Hernacki is an architect in Symantec Research Labs, where he works with a dedicated team to develop future technologies. Hernacki has more than 10 years of experience with computer security and enterprise software development. He has conducted research and commercial product development in a number of security areas, including intrusion detection and analysis techniques, honeypots, and wireless and mobile technologies. Hernacki earned a bachelor's degree in computer engineering, with honors, from the University of Michigan.

Brian wrote Chapter 11 (Mobile Malicious Code Mitigation Measures).

Jose Andre Morales is a Ph.D. graduate in computer science from Florida International University in the research area of computer virus detection based on identifying self-replication. He focuses on detecting viruses in mobile devices and develops antivirus solutions. He is a member of Sigma Xi, Upsilon Phi Epsilon, ACM and IEEE. He is also the cofounder of the Computing Hispanic Ph.D. Mailing List.

Jose wrote Chapters 3 (Timeline of Mobile Malicious Code, Hoaxes, and Threats), 4 (Overview of Malicious Mobile Code Families), and 5 (Taxonomy of Mobile Malicious Code).

Craig Wright is associate director, risk advisory services at BDO Kendalls (NSW-VIC) Pty. Ltd. He has authored numerous IT security-related articles and books. He also has designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory. He designed and managed the implementation of many of the systems that protect the Australian Stock Exchange as well as the security policies and procedural practices within Mahindra and Mahindra, India's largest

vehicle manufacturer. The Mahindra group employs over 50,000 people in total and has numerous business interests from car to tractor manufacturing to IT outsourcing. Craig is one of the few people with a GSE certification and the first in the compliance stream. He has 27 GIAC certifications and is working on his eighth GIAC Gold paper.

Craig wrote Chapter 9 (Forensic Analysis of Mobile Malicious Code).

Acknowledgments/Contributors

The authors of this book want to thank multiple individuals, lists, and private sources within the computer security industry for their ongoing support and development of mobile malicious code products and services. The following individuals significantly contributed to content within this book as noted for each:

Collin Mulliner is a programmer, hacker, and a full-time security researcher. Collin's main area of research is the security of mobile devices and networks with a special emphasis on mobile and smartphones. In recent years Collin was doing a lot of research and development on Bluetooth. He created the first Bluetooth port scanner. Since 1997, Collin has done projects for most of the existing mobile device platforms. In 2006, Collin received a master's in computer science degree from the University of California, Santa Barbara.

Collin wrote sections on MMS, Palm, and J2ME in Chapter 7.

Ralf Hund is a master's candidate in mathematics and computer science at the University of Mannheim, Germany. As a student helper at the Laboratory for Dependable Distributed Systems, he has completed work that includes the development of a sandbox for the Windows Mobile platform. He has a special interest in practical aspects of IT security (e.g., software security, static malware analysis, and dynamic malware analysis).

Ralf has more than 10 years of experience in reverse engineering and programming on Windows and Linux operating systems, with a special focus on low-level details.

Ralf wrote the technical sections of Chapter 8 on behavioral analysis of MMC.

Additional individuals we would like to thank for helping in technical review include Mikko H. Hypponen, Fred Doyle, Joep Gommers, and Josh Murray.

Contents