Seven Deadliest USB Attacks

Syngress Seven Deadliest Attacks Series

Seven Deadliest Microsoft Attacks
ISBN: 978-1-59749-551-6
Rob Kraus

Seven Deadliest Network Attacks
ISBN: 978-1-59749-549-3
Stacy Prowell

Seven Deadliest Social Network Attacks
ISBN: 978-1-59749-545-5
Carl Timm

Seven Deadliest Unified Communications Attacks
ISBN: 978-1-59749-547-9
Dan York

Seven Deadliest USB Attacks
ISBN: 978-1-59749-553-0
Brian Anderson

Seven Deadliest Web Application Attacks
ISBN: 978-1-59749-543-1
Mike Shema

Seven Deadliest Wireless Technologies Attacks
ISBN: 978-1-59749-541-7
Brad Haines

Visit **www.syngress.com** for more information on these titles and other resources

Seven Deadliest USB Attacks

Brian Anderson

Barbara Anderson

Technical Editor **Andrew Rabie**

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS®

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

Seven Deadliest USB Attacks
© 2010, Elsevier, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: *www.elsevier.com/permissions*.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Anderson, Brian (Brian James)
Seven deadliest USB attacks / Brian Anderson ; technical editor, Barbara Anderson.
p. cm.
ISBN 978-1-59749-553-0
1. Computer security. 2. Computer networks–Security measures. I. Title.
QA76.9.A25A52 2010
005.8–dc22

2010008745

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-553-0

Printed in the United States of America
10 11 12 13 14 10 9 8 7 6 5 4 3 2 1

Elsevier Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

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

For information on all Syngress publications visit our Web site at *www.syngress.com*

Working together to grow libraries in developing countries
www.elsevier.com | www.bookaid.org | www.sabre.org
ELSEVIER BOOK AID International Sabre Foundation

Contents

A preview chapter from *Seven Deadliest Social Network Attacks* can be found after the index.

About the Authors

Lead Author

Brian Anderson (MCSE) is an independent security consultant specializing in multiple disciplines. Brian began his security career with the USMC serving as a military police officer while participating in the Somalia humanitarian efforts and also served multiple tours of duty in the Middle East and Korea. Additionally, he served as an instructor for weapons marksmanship, urban combat, and less than lethal munitions.

Brian's technical experience began when he joined EDS as an associate. Here, he became part of a leveraged team specializing in infrastructure problem resolution, disaster recovery, and enterprise design. His career progression was swift, carrying him through security engineering and into architecture and earning himself lead roles throughout. Brian was a key participant in many high-level security projects driven by HIPAA, PCI, SOX, FIPS, and other regulatory compliance projects. In these projects, his roles included support, design, remediation, and consultation for infrastructure dependent services, multitenant directories, IdM, RBAC, SSO, WLAN, data encryption, leveraged perimeter design, and security strategies.

Technical Editor

Andrew Rabie is an Executive Ninja with Attack Research. Attack Research is a global information security think tank that focuses on full disclosure of actual and real security threats. His role includes proactive defensive strategies and risk mitigation to an ever-increasing offensive trend in today's security world.

He currently resides in the middle of the Irish Sea on the Isle of Man, with his wife Leslie.

Contributing Author

Barbara Anderson (CCSP, CISSP, CCNP, CCDP) has worked in the information technology industry as a network and server security professional for over 11 years. During that time, she has acted as a senior network security engineer, providing consulting and support for all aspects of network and security design. Barbara comes from a strong network security background and has extensive experience in enterprise design, implementation, and life-cycle management.

Barbara proudly served her country for over 4 years in the US Air Force and has enjoyed successful positions at EDS, SMU, Fujitsu, ACS, and Fishnet Security. These experiences and interactions have allowed her to become an expert in enterprise security, product deployment, and product training.

Introduction

INFORMATION IN THIS CHAPTER

- Book Overview and Audience
- Organization and Orientation
- Emphasis on Risk

BOOK OVERVIEW AND AUDIENCE

While hardware thefts and network-based vulnerabilities always seem to take the front seat in the minds of security strategists and business executives, physical attacks against personal area networks (PANs) have been growing in variety, simplicity, and severity. Universal Serial Bus (USB) attacks top these concerns due to wide adoption and because they are nearly effortless to build, deploy, and execute. When combined with the U3 or other portable platform technologies, they leave minimal if any indication of an infiltration. It is no longer necessary for a malicious insider to risk being caught accessing unauthorized data stores or stealing computer equipment. Instead, he or she can just borrow resources for instant gratification with minimal risk of being discovered or disciplined.

This book was written to target a vast audience including students, technical staff, business leaders, or anyone seeking to understand fully the removable-media risk for Windows systems. It will provide you with the tools, tricks, and detailed instructions necessary to reconstruct and mitigate these activities while peering into the risks and future aspects surrounding the respective technologies.

The attacks outlined in this book are intended for individuals with moderate Microsoft Windows proficiency. Live Linux operating systems will be used in Chapter 5, "RAM dump," and Chapter 7, "Social Engineering and USB Come Together for a Brutal Attack"; however, thorough documentation is provided for those unfamiliar with these operating systems. A U3 SanDisk Cruzer, Lexar flash drives, iPod, and iPhone are the hardware platforms employed to launch the attacks in this book.

ORGANIZATION AND ORIENTATION

Although the scope of this book is limited to Windows systems and the USB avenue, each chapter focuses on a different approach. It is not necessary to start from the beginning and read it in its entirety, although some of the sections relate to other chapters. Cross-references are included in respective chapter sections where pertinent subject matter may apply. While Windows systems are in the spotlight here, Mac, Linux, and UNIX systems are equally susceptible to similar attacks.

Microsoft uses the removable-media reference in their technical documentation,[A] and since a majority of the attacks are likely to occur on these systems, it has been adopted for orientation in this book. Removable media is any storage media that is designed to be removed from the host while it is still powered on. Tapes, compact discs (CD), digital versatile disks (DVD), solid-state drives (flash drives, SD, MMC, and others), and hard disks top a long list that qualify for this categorization. While this book will focus primarily on external flash and disk drives, the others should not be fully excluded as potential attack-packing apparatuses. The following sections will highlight the contents of each chapter to help you understand why these were chosen as the seven deadliest attacks.

Chapter 1 "USB Hacksaw"

The USB Hacksaw takes a completely new approach to data compromise. It combines several utilities that already exist in the wild to render an intriguing data-retrieval solution. Microsoft's recent updates and statements surrounding autorun behaviors are explained to present a detailed look into its response regarding these recent threats. Various portable platform technologies will also be described to show how USB flash drives are evolving into the next generation of virtual and fully functional operating environments.

Chapter 2 "USB Switchblade"

In this chapter, we will examine the USB Switchblade that was originally designed to aid administrators or auditors in gathering information for Windows systems. The modular design and ease of use make it a potentially devastating tool when placed in the wrong hands. Windows and common program-hardening recommendations are supplied to help combat these potential perpetrators.

Chapter 3 "USB-Based Virus/Malicious Code Launch"

USB and viruses has been a hot topic in the media as of late, and this chapter investigates these outbreaks and provides the most reasonable protective measures that can be applied. Malicious code categorizations and definitions are supplied to help you stay current in this fast-paced field of intrusive software. Documentation is

[A] www.microsoft.com/whdc/archive/usbfaq.mspx

also included to create a basic infection injected by a USB flash drive to show how easily this can be accomplished.

Chapter 4 "USB Device Overflow"

In Chapter 4, we will provide you with a real-world example of USB-based heap overflow, which was unveiled by researchers at a Black Hat conference to gain administrative access to a Windows system. The physical and logical tools necessary to devise such an attack are explored to illustrate a theoretical recreation of their device. Additional situations are provided to show how USB and overflows are commonly used to exploit a number of different devices.

Chapter 5 "RAM dump"

Chapter 5 delves into the evolution of forensics in computer security. The Princeton cold-boot attack will be demonstrated to show the effectiveness of USB devices and how disastrous the consequences can be if the tables are turned. Active and image-based memory analysis is a growing field due in large part to the recent developments of memory-resident malwares and full-disk encryption schemes. An entire suite of tools is supplied with additional procedures to facilitate memory acquisition and analysis.

Chapter 6 "Pod Slurping"

The technique known as *pod slurping* derives its name from the media-player market frenzy, but more specifically Apple's iPod. In this chapter, we will uncover the speculation, provide a practical example, and discuss the defensive measures needed to mitigate these attacks. Additional instructions are included to illustrate a situation involving current technology, which can be used to silently siphon sensitive data out of a corporate environment.

Chapter 7 "Social Engineering and USB Come Together for a Brutal Attack"

This chapter will peer into the human element of security to demonstrate just how susceptible each of us is. We will also discuss the risks, rewards, and controversy surrounding social-engineering engagements and describe what you need to know regarding each. The premier penetration-testing platform known as Backtrack 4 will be the highlight, although combining all of the attacks in this book will bestow the most brutal assault.

EMPHASIS ON RISK

National Institute of Standards and Technologies (NIST) publication 800-12 provides an excellent description of computer security, which states "the protection afforded to an automated information system in order to attain the applicable

objectives of preserving the integrity, availability, and confidentiality of information system resources (this includes hardware, software, firmware, information/data, and telecommunications)."[1] Confidentiality, integrity, and availability are extremely vulnerable for the systems and environments susceptible to these types of attacks. Included below is a short list of data types these specific attacks can acquire by leveraging a removable-media device.

- Exposure of data for keys or secrets housed in encryption software, products, services, external/portable drives, systems, networks, and applications
- Passwords of Outlook PST files, Remote Desktop Protocol (RDP) connections, File Transfer Protocol (FTP), Virtual Network Computing (VNC), virtual private network (VPN), dial-up configurations, mapped network drives, Windows domain credentials, browser AutoComplete fields, protected storage items, and much more.

These are just the tip of a huge iceberg full of cold-hearted malevolent activities that can intrude on your business, everyday life, and well-being. USB flash memory devices are on the forefront of the proximity attack vector, and their enormous capacities have only increased the amount of damage they can inflict.

SUMMARY

Localized attacks are not new to the threat landscape. Corporate industries and government agencies have been well aware of these issues for quite some time now. These problems continue to fluster security professionals as they scramble to update policies, procedures, and environments to minimize the impact these types of attacks can impose.

There are a number of software vendors who provide enterprise-level mechanisms to protect against the variety of assaults designed against PANs. This is good news for those who can afford their hefty price tags and complex integration schemes. Unfortunately, small businesses, educational facilities, consumers, and other undersized entities are left to defend themselves by whatever means they have available. The defensive sections in this book will outline the most reasonable mitigations that should be taken into consideration. While these may not completely rid your environment of all potential dangers, they will significantly hinder the attacks covered in this book.

Endnote

1. http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1.html. Accessed September 2009.