Executing Windows Command Line Investigations

"This book opens a world of Windows command line functionality that investigators never knew existed. Through the use of real world examples and logical application scenarios, the authors have created a must have tool for every forensic examiners kit." – Anthony Martino, Director, Northeast Cybersecurity and Forensics Center

Executing Windows Command Line Investigations

While Ensuring Evidentiary Integrity

Chet Hosmer
Joshua Bartolomie
Rosanne Pelli

ELSEVIER

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
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, USA

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
A catalog record for this book is available from the Library of Congress

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

ISBN: 978-0-12-809268-2

Publisher: Todd Green
Acquisition Editor: Chris Katsaropoulos
Editorial Project Manager: Anna Valutkevich
Production Project Manager: Mohana Natarajan
Cover Designer: Mark Rogers

Typeset by Spi Global, India

Dedication

Chet Hosmer
To my Mom, for sharing your love of reading with me.

Joshua Bartolomie
To my beautiful wife Dawn and two amazing daughters Kaylee and Alyson. Thank you for always supporting, and putting up with, me and for inspiring me to always strive to be the best person I can be. To my parents Marjorie and Joseph, who taught me to never limit myself and to not take life too seriously and enjoy it as much as possible, because no one ever gets out of it alive.

Rosanne Pelli
To my husband Frank and my children Frankie and Sophia, thank you for my amazing life! To my parents who always taught me to "go big or stay at home" and to Fred Demma, thank you for giving me my first opportunity in this field and challenging me every day!

Finally, I would like to dedicate this book to the men and women who have worked countless hours in developing cutting-edge cyber technologies, investigating cyber incidents, and protecting our critical infrastructure. Thank you!

Software Download Instructions

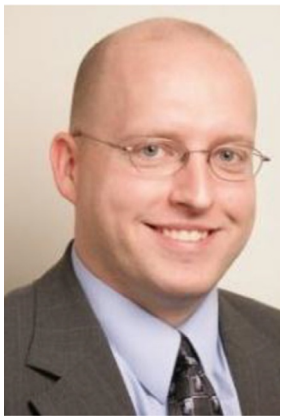
To download the companion PIRCS software, please visit http://booksite.elsevier.com/9780128092682/

Biography

Chet Hosmer is the founder of Python Forensics, Inc., a non-profit organization focused on the collaborative development of open-source investigative technologies using the Python programming language. Chet serves as a visiting professor at Utica College in the Cybersecurity Graduate Program where his research and teaching focus on advanced steganography/data hiding methods and related defenses. He is also an Adjunct Faculty Member at Champlain College in the Master of Science in Digital Forensic Science Program where he is researching and working with graduate students to advance the application Python to solve hard problems facing digital investigators.

Chet makes numerous appearances each year to discuss emerging cyber threats including appearances in National Public Radio's Kojo Nnamdi show, ABC's Primetime Thursday, NHK Japan, and ABC News Australia. He is also a frequent contributor to technical and news stories relating to cyber security and forensics and has been interviewed and quoted by IEEE, The New York Times, The Washington Post, Government Computer News, Salon.com, DFI News, and Wired Magazine.

He is the author of three recent Elsevier/Syngress Books: *Python Passive Network Mapping*: **ISBN-13:** 978-0128027219, *Python Forensics*: **ISBN-13:** 978-0124186767, and *Data Hiding* which is co/authored with Mike Raggo: **ISBN-13:** 978-1597497435. Chet delivers keynote and plenary talks on various cyber security related topics around the world, each year.



Joshua Bartolomie (CISSP, CRISC, DFCP, CEECS, CFCE) has 20 years of technical and management experience within the information technology and cyber security domains. Joshua has contributed to and established programs that range from teaching digital forensics to designing, implementing, and evolving cutting edge Security Operations Centers, Incident Response Teams, and Cyber Security Architecture Organizations. Joshua is an active participant in multiple information sharing and collaborative consortiums and has presented at numerous cyber security forums, conferences, and venues.

In his current role, Joshua is responsible for translating corporate business strategies, environmental conditions, infrastructure requirements, and industry best practices into strategic cyber security designs and architectural roadmaps. Joshua holds a Master's Degree in Information Assurance from Norwich University and a Bachelor's of Science in Digital and Computer Forensics from Champlain College.

Rosanne Pelli, is a certified Project Management Professional through the Project Management Institute and CompTIA Security+ professional with Harris Corporation. She has over 10 years of experience in the coordination, programmatic oversight, and management of US government contracts as well as Harris' Secure-U Training Program. During her years of experience, Rosanne has assisted in the management and coordination of various government contracts that focused on the identification and analysis of emerging cyber threats; evaluation and transition of cyber security technologies for tactical use by the cyber security community; technical assistance to federal, state, and local law enforcement communities; development and maintenance of a virtual cyber security training portal; and the development, coordination, and execution of various national and international cyber security training initiatives.

Foreword

Over the course of my 18-year career in computer security, I have never before seen as big a gaping hole in our industry, begging for skilled computer security talent, as we have now. The lack of talent and the failure of technology to optimally equip the skilled resources we employ, have led organizations to suffer material breaches and spend millions of dollars to respond to and recover from those breaches.

The threat landscape continues to grow in sophistication and breadth of scope. Numerous high-profile breaches involving well-known corporations and government entities have been spotlighted by the media. Most of these breaches being compromised through the targeting of employees or unpatched computer systems. While this is still true, the explosion of the Internet of Things and embedded devices has considerably broadened the threat landscape, often doubling or tripling the possible targets and attack vectors available to the threat actor today. In addition to the explosive growth of targets and attack vectors, there is also substantial growth in the number of threat actors themselves. The relative ease of operating a nefarious cyber business is alarming. Malicious code is readily available and is bought and sold on a market. The use of online payments, such as Bitcoin, make it seemingly impossible to trace back.

In today's world, it is generally not a matter of if but when an attacker breaches your environment. After all, we have to protect against everything while the attacker only has to find one thing. As such, the focus of cyber security has shifted from prevention to detection and response. A skilled incident responder or forensics expert can make the difference between having a full-scale breach on your hands and stopping a compromise early in the attacker lifecycle by proactively hunting and analyzing attacks in flight. Incident response and forensics is considerably more than being able to operate expensive tools and administer systems. It is about understanding all aspects of the attacker, their techniques, the lifecycle of a compromise, and the ability to investigate and uncover evidence or indication of compromise every step of that life cycle and do so while maintaining full integrity of the data and the investigation.

Incident Response and forensics are about the depth-of-knowledge and the attention to detail. A highly skilled responder is worth his or her weight in gold and can make the difference between your company being highly successful or finding itself on the cover of the Wall Street Journal, immortalized as yet another victim of a high-profile data breach.

Josh, I would like to personally thank you for passing your immense talent and experience in the area of forensics and incident response forward into a community and world that desperately need it. There are more jobs available today than skilled resources available to fill them; meaning that there are too many organizations ill equipped, under prepared, vulnerable, and unprotected. I look forward to seeing

our industry continue to invest and make advancements in the people, process, and technology needed to defend and protect our corporations and our government. I also look forward to seeing this book help educate and train the next generation of cyber security warriors.

James Carder
CISO & VP, LogRhythm Labs

Preface

Tim Patterson and Seattle Computer Products, headquartered in Seattle, WA, USA, made the first release of 86-DOS which was designed to run on an Intel 8086 Computer Kit in Aug. of 1980. Microsoft, headquartered in Redmond, WA, USA, purchased 86-DOS from Seattle Computer Products and hired Tim Patterson later that year. In Aug. of 1981 IBM, headquartered in Armonk, NY, USA, released PC-DOS 1.0, which was developed and owned by Microsoft. IBM insisted that Microsoft retain title and ownership of the product to avoid possible legal issues regarding software infringement. In hindsight many have questioned this decision by IBM which eventually resulted in the evolution of Microsoft as one of the largest software companies in the world.

Within a year after the release of PC-DOS 1.0, Microsoft licensed their version of MS-DOS to hundreds of companies as a general purpose operating system that could run on a wide variety of Intel 8086 based computers. This gave rise to a whole new generation of IBM compatible computers over the next decade. Even early 16-bit versions of Microsoft Windows ran as a Graphical User Interface on top of MS-DOS.

Microsoft still provides an MS-DOS *like* interface today, delivered as the software application *cmd.exe*. This application provides a more direct communication between user entered commands and the underlying operating system. Many consider this a nongraphical command shell where you can run built-in commands or third-party character based applications.

Many investigators and examiners today rely on this "more direct interface" with the operating system to interrogate Microsoft Windows based systems in either live or postmortem scenarios.

This book explores three critical areas. First, to assess the viability of using this command based interface when investigating or examining live systems. Second, to examine the criticality and volatility of evidence integrity. Third, to explore and demonstrate the use of PIRCS (Proactive Incident Response Command Shell) to enhance live investigations. The PIRCS technology provides a Windows Command Line (CLI) *style* interface combined with a secure evidence repository. PIRCS provides a framework for maintaining evidence integrity, validating evidence collection methods, preserving the investigative process, and providing nonrepudiation of actions taken by investigators when interacting with the command line.

The book is applicable to a wide audience and includes a copy of the PIRCS technology to enable experimentation and undergraduate and graduate studies, along with incident response and live investigation applications. The authors of the book and the developers of the technology encourage your comments and suggestions to help advance command line based investigation technologies.

Acknowledgments

Chet Hosmer

Dr. Gary Kessler, the technical editor for this book. Gary's knowledge, guidance, and insight always enhance every chapter.

Chris Katsaropoulos, Anna Valutkevich, and the whole team at Elsevier for your enthusiasm for this topic, and for all the guidance, patience, and support along the way.

To Janet for your encouragement and insightful suggestions on how to make the material accessible by everyone. I want to thank Rosanne and Josh for their collaboration on this book. Their insight, attention to detail and deep subject matter knowledge added significant value to all aspects of the book.

Joshua Bartolomie

To Chet Hosmer and Rosanne Pelli, for all of their hard work and continued drive to ensure this book saw the light of the day and was the best it could be.

To James Carder, thank you for your contribution to this book and for the many years of support, collaboration, and friendship.

Lastly I would like to thank all of the practitioners that continually work to advance the digital forensics and incident response field and who share their knowledge, tools, and methodologies. We would not be where we are today without all of your insights and expertise.

Rosanne Pelli

The Proactive Incident Response Command Shell (PIRCS) technology was based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD), BAA 11–02 and Air Force Research Laboratory Information Directorate via contract number FA8750-12-C-0271.[1]

I am extremely grateful to the many practitioners who took the time out of their busy work schedule to discuss their requirements and provide feedback to the PIRCS technology. Also, a special thanks to all the folks within Harris Corporation who supported this project.

To Joshua Bartolomie whose expertise and innovative spirit led to the PIRCS concept and to Chet Hosmer, my sincere gratitude for your patience, support, and guidance, without you this book would not be a reality. Thank you!

[1]The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DHS, Air Force Research Laboratory, or the US Government.

Harris Corporation

Harris Corporation, headquartered in Melbourne, FL, USA, is a leading technology innovator, solving its customers' toughest mission-critical challenges by providing them solutions that connect, inform, and protect. Harris supports customers in more than 125 countries, has approximately $8 billion in annual revenue, and 22,000 employees worldwide. The company is organized into four business segments: Communication Systems, Space and Intelligence Systems, Electronic Systems, and Critical Networks. For more information on Harris Corporation, visit www.harris.com.

CHAPTER

The impact of Windows Command Line investigations

1

triage: Word Origin
1727 from the French triage "a picking out, sorting" From Old French approximately 14 Century, trier "to pick or cull". During World War I, triage *was the adopted term for sorting the wounded into groups according to the severity of their injuries.*

CHAPTER OUTLINE

INTRODUCTION

As cybercrime activities continue to expand at an alarming rate, our response to these events must keep pace. Reports similar to the following can be found over and over again:

> *According to TrendMicro's 2014 Security Roundup, "2014 was the year of mega breaches, hard-to-patch vulnerabilities, and thriving cybercriminal underground economies. It encapsulated threats of grand proportions, the consequences of which set companies back billions in losses and consumers an unknown figure in lost or stolen personally identifiable information (PII).*
>
> *It was in 2014 when the world witnessed the largest reported hack that led to a staggering loss of around 100 terabytes of data and up to $100 M damages for Sony Pictures Entertainment Inc. (SPE). "Unprecedented in nature" and "an unparalleled and well planned crime" were but a few phrases that described*

Executing Windows Command Line Investigations. http://dx.doi.org/10.1016/B978-0-12-809268-2.00001-8

the Sony Pictures breach in an internal memo released to its employees. This reminds IT professionals of the crucial role that a layered, customized defense plays inside very large networks."

CYBERCRIME METHODS AND VULNERABILITIES

In addition to the increase in cybercrime activities, specific classes of cyber criminals are changing the landscape for both forensic investigation and incident response. Just a few key examples of some current terms:

Cyber Terrorism

Any use of Information and Communication Technology to attack civilian systems in order to intimidate, coerce, or destroy government or societies as a way to advance political, religious, economic, or ideological goals.

Dr. Gary Kessler, 2016.

Hacktivism: The act of breaking into organizational infrastructures for a politically, socially, or terrorist motivated purpose is now becoming a popular method of shaping political debates. This has changed slightly over the past several years as "anonymous" has become less active mainly due to internal divisions. Sony Pictures was the most visible target in recent years, and collecting specific evidence and performing triage in the face of these attacks is still debated today. When such attacks occur it is possible to react such that valuable evidence is lost or compromised. Through the use of triage best practices along with the skillful use of technology, investigators can collect valuable evidence while preserving the integrity of such evidence. In addition, the immediate collection of host and network activity may help to mitigate an attack and quarantine systems and networks from further damage.

Extortion and ransomware: Various forms of cyber extortion and new ransomware scams have emerged. In one of the most publicized cases, the computers of Miss Teen USA, Cassidy Wolf, along with several other young women in southern California were hacked by Jared James Abrahams. He then took control of the victim's webcam and secretly photographed them, demanding nude photographs from the victims. He pled guilty and is serving 18 months in Federal Prison. This has defined the new term, "sextortion."

Businesses and organizations are not exempt from this activity and are being targeted by extortionists as well. The most common approach is to breach an organization network and steal sensitive and personal identifiable information (PII). The extortionist then demands a ransom payment in exchange for not releasing or selling the "exfiltrated" data. In many cases they demand bitcoins and other virtual currencies as payment, allowing the entire transaction to occur in the cyber world. In both of these examples rapid response and triage of evidence from the victim's computers and networks is vital. Another form of ransomware, of course, is like Cryptolocker, that locks files unless you pay for a key … from "companies" that have a help desk and actually give you the key if you pay the ransom. Worse is that many

organizations—including at least one police department (Tewksbury, Massachusetts)—have paid the ransom in order to get their files back!!

Cyberbullying, harassment, and stalking: There are both Federal and State Laws that now provide penalties for those engaged in such actions: The Federal stalking statute, 18 USC Section 2261A, was amended to include the use of an "interactive computer service" to "engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to," the victim or a member of the victim's family. The statute requires that the defendant physically travel across state lines, making it inapplicable to many cyberstalking cases. To counter this, almost all States now include laws against cyberstalking, cyberharassment, and cyberbullying. Some states have created new laws, while others have modified harassment or stalking statutes to include cyber. In any case, the timely collection of evidence from victims or potential victim's computers is critical in order to prevent harm and to prosecute those perpetrating the harassment, bullying, or stalking.

Crimes against children: The Internet Crimes Against Children (ICAC) Task Force was created to help Federal, State, and Local law enforcement agencies enhance their investigative responses to offenders who use the Internet, online communication systems, or computer technology to sexually exploit children. Since the perpetrators of such activities have become more sophisticated and elusive, our ability to collect and examine evidence from potential victims, computers, and recent network activity is vital in identifying and tracking those involved. In many cases this needs to be accomplished using triage methods and cannot wait for the backlog processing of computer evidence. In addition, since the parents and guardians typically own the computer systems in use by the minor victims, with their permission first responders can legally access electronic evidence in order to begin triage operations.

Sophisticated botnets: Botnets remain one of the hacker's most relied upon weapons. This malicious software is at the forefront of spamming, distributed denial of service attacks and coordinated hacking activities. One of the most recent additions is "ZeroAccess," said to be controlling over 2 million unsuspecting computers world-wide. The bot "Storm" is estimated to control as many as 50 million computers and operates on a peer-to-peer basis removing the need for a centralized bot herder, making it more difficult to shutdown. In many cases bots (or more specifically their zombie counterparts), exist only in memory and when systems are shutdown traces of the zombie are very difficult to detect. Thus examination of the running state of computer systems using forensic triage of memory and active processes is a vital step in identifying and defeating these threats.

NOVEL VULNERABILITIES

The latest vulnerabilities add yet, another dimension to incident response requirements and forensic triage, not seen before. These require specials tools, technologies, and methods that in many cases require command line level operation and setup. A few examples include:

Heartbleed: is a vulnerability in the OpenSSL software library (notably not a protocol flaw but caused by a coding error) that when exploited can provide hacker access to the memory of data servers. It has been estimated that over a million websites could have been affected and many more applications utilizing OpenSSL. Information contained in the exploited memory could include sensitive data including usernames, passwords, sensitive documents, and a cadre of PII. This vulnerability under certain conditions may reveal the server's private key causing the necessary revocation of server based certificates. Fig. 1.1 depicts the number of revoked certificates in the days following the announcement of the Heartbleed bug.

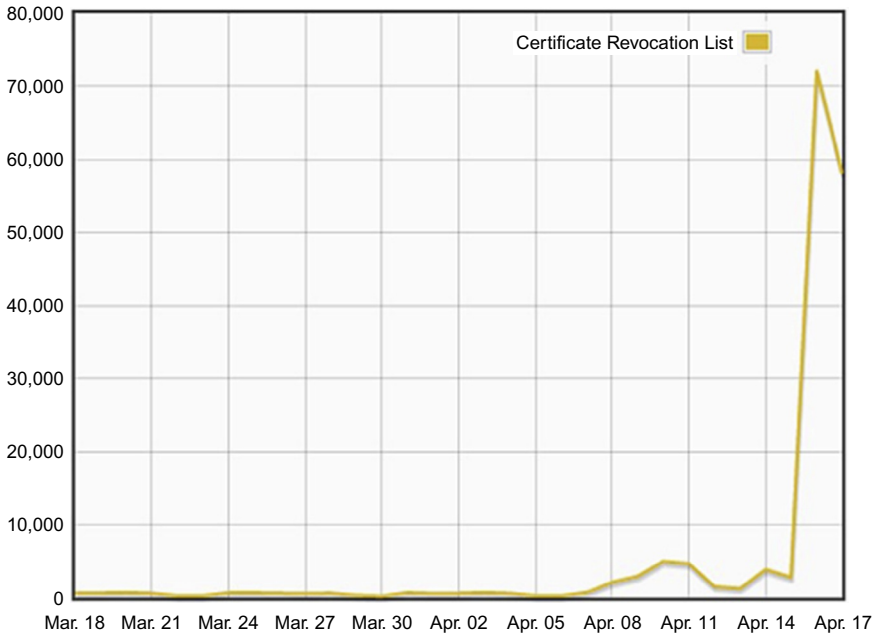


FIG. 1.1

Heartbleed bug catalyst for massive certificate revocations.

POODLE attack vulnerability: POODLE is a design vulnerability found in the way SSL 3.0 handles block cipher mode padding. The POODLE attack allows an attacker to exploit the vulnerability to decrypt and extract information from inside an encrypted transaction. The direct impact is the potential for an attacker to steal a server's digital keys used in encrypted communications and the protection of proprietary internal documents.

Windows XP (zero-day-forever, now that XP is end of life): It is estimated that as many as 31% of home and enterprise computers are still running the Windows XP operating system today. As of Apr. 8, 2014, support and updates for Windows XP has ended leaving these systems vulnerable to exploitation. In addition, leaked versions

of the Windows 2000 operating system source code (much of which is shared with Windows XP) gives hackers an avenue to identify and then exploit vulnerabilities in the most tightly held source code base.

In addition, zero-day vulnerabilities continue to impact Microsoft Windows platforms. Fig. 1.2 depicts the timeline of 2014 events as reported by TrendMicro.

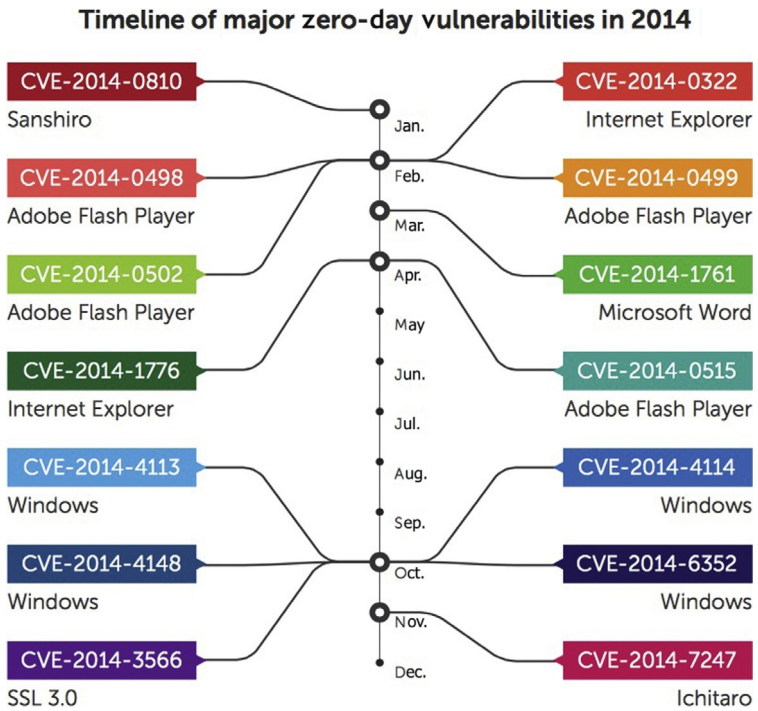


FIG. 1.2

2014 zero-day vulnerability timeline.

Zero-Day Vulnerabilities "any vulnerability that is exploited prior to anyone (other than the attacker) knowing about the vulnerability."

Common vulnerabilities and exposures (CVE) is a dictionary or catalog of known security threats.

CYBER CRIMINALS USE THE WINDOWS COMMAND LINE

Microsoft Windows based systems continue to dominate the landscape and it is no secret that cyber criminals leverage the Windows Command Line (Fig. 1.3) when infiltrating these devices. As we have identified, both cybercrime methods and