CYBERCRIME AND ESPIONAGE
CYBERCRIME AND ESPIONAGE
An Analysis of Subversive Multivector Threats

WILL GRAGIDO
JOHN PIRC

RUSS ROGERS, Technical Editor
Contents

Foreword ................................................... ix
Preface .................................................... xi
Acknowledgments .......................................... xiii
About the Authors ............................................. xv

Chapter 1 Cybercrime and Espionage and the New Security 101 .............................................. 1
Introduction .................................................. 1
He Who Does Not Prevent a Crime When He Can, Encourages It ................................... 2
What’s Old Is New Again ........................................ 3
A Changing World ............................................. 7
Cybercriminal Statistics: U.S. and Abroad .................................. 8
The Statistics of Cybercrime .................................. 9
Separating the Wheat from the Chaff: Qualifying Amateurs and Professionals .................. 10
Trends in 2011 ............................................. 13
Myopic to the Catastrophic: Advanced Persistent Threats .................................. 16
Points of Confluence: Events That Have Shaped the Future of Privatized Cybercrime and Espionage .................................. 18
Agendas in Next Generation Cybercriminal Activity .................................. 19
The Coming Decade ............................................. 19
Summary .................................................. 20

Chapter 2 Evolution Revolution ............................................. 21
Introduction .................................................. 21
Communication ............................................. 21
Criminal Activity ............................................. 27
Summary .................................................. 33

Chapter 3 The Silent Killer: How Regulatory Compliance Has Worsened The State of Information Security .................................. 35
Introduction .................................................. 35
Regulatory Compliance Telemetry .................................. 36
Transborder Data Flow Restrictions .................................. 36
ISO Security Standards ............................................. 40
Health Insurance Portability and Accountability Act (HIPAA) .................................. 41
Chapter 7  Cyber X: Criminal Syndicates, Nation States, Subnational Entities, and Beyond ...................... 115
    Introduction ............................................. 115
    Classifying the Cyber Actor ................................ 116
    Attack Sophistication Model ................................ 117
    Modus Operandi ........................................... 120
    The Importance of Attribution ................................ 121
    Criminal and Organized Syndicates ......................... 123
    Nation States ............................................. 127
    Subnational Entities ........................................ 128
    Summary ...................................................... 131
    References .................................................... 132

Chapter 8  The Rise of the Subversive Multivector Threat ................................................................. 135
    Introduction ............................................. 135
    Sun Tzu and *The Art of War* ................................ 135
    Defining The Subversive Multivector Threat (SMT) ............. 139
    Summary ...................................................... 150

Chapter 9  Seven Commonalities of Subversive Multivector Threats ..................................................... 153
    Introduction ............................................. 153
    Seven Commonalities of Subversive Multivector Threats ........... 153
    Five Names in Threats You Should Know ......................... 161
    Next-Generation Techniques and Tools for Avoidance and Obfuscation .................................................. 173
    Summary ...................................................... 174
    References .................................................... 175

Chapter 10  Examples of Compromise and Presence of Subversive Multivector Threats ............................... 177
    Introduction ............................................. 177
    Black, White and Gray: Motives and Agendas of Cyber Actors with Respect to Cybercrime and Espionage .............. 178
Onion Routed and Anonymous Networks ................................................. 186
WikiLeaks .......................................................................................... 191
Project Aurora .................................................................................. 195
Summary ............................................................................................ 196

Chapter 11  Hiding in Plain Sight: Next-Generation Techniques
and Tools for Avoidance and Obfuscation ............................................ 197

Introduction ...................................................................................... 197
Malware Quality Assurance Testing .................................................... 198
IP Attribution ...................................................................................... 211
IP Spoofing ......................................................................................... 217
Summary ............................................................................................ 222
References .......................................................................................... 222

Chapter 12  Weapons of Our Warfare: Next-Generation
Techniques and Tools for Detection, Identification,
and Analysis ...................................................................................... 223

Introduction ...................................................................................... 223
Legacy Firewalls ................................................................................ 224
Antivirus ............................................................................................. 225
Intrusion Detection Systems and Intrusion Prevention Systems .......... 226
What Is in a Name? ........................................................................... 226
MOSAIC ............................................................................................ 229
Advanced Meta-Network Security Analysis .................................. 234
Next Generation Security Framework ............................................. 236
Summary ............................................................................................ 245
References .......................................................................................... 245

Index ................................................................................................. 247
FOREWORD

You will find this an interesting book; it covers a lot of ground, but pulls the information together in the end. *Cybercrime and Espionage* opens with a quote from Cicero from the first century B.C. The discussion of fraud and justice reaches back to the code of Hammurabi and a page later we read about the Smartphone. There are a few dominant themes:

- The authors work diligently to build a strong foundation based on history to show us, while the technology is new. There is an unprecedented amount of information that shows that crimes we are exposed to are not so new; nothing about the iPad changes human behavior.
- The authors have worked at advanced security companies and have access to the actual tools and attacks that are being used by criminals, Nation States, and organized groups to capture and exploit information.
- Knowing that the technology will continue to change, the authors have developed frameworks to help clarify this complex information.
- Case studies and actual examples, many of which went to court, are shared so that it is clear this is not opinion but what is actually happening.

With these themes in mind, do not be surprised if the discussion ranges from the Greek alphabet, the printing press, the history of the ARPANET, and the public switched network and then to the cutting-edge work of Bond and Danezis and why we fall prey to malware again and again. The discussion on compliance not equaling security is as clearly stated (and supported) as any I have seen, and this is such an important concept to understand because if you follow the money, a lot is invested in compliance. We are shown that physical and logical security are becoming less and less related. Two examples of why this can be a problem are the stories of Dong Chul Shin and Danielle Duann; both had insider access and were terminated from their organizations but were able to access IT resources via their organizations' VPN.

Chapter 6 is particularly chilling, this is where the authors cover state-sponsored information gathering, and they do not hold back. They remind us again this is not a new problem; human nature has not changed, and their poster children include Ethel and Julius Rosenberg, Klaus Fuchs, Clayton Lonetree, Aldrich Ames, and Clyde Lee Conrad. This is followed
by a veritable who’s who of significant groups, perhaps smaller than Nation State, involved in harvesting and exploiting information.

_Cybercrime and Espionage_ also goes into some considerable depth to explain exactly how the criminal underground is able to harvest information about people like you or I. I haven’t seen this much explanatory information since _Crimeware_. We learn about the Advanced Persistent Threat, and rather than throwing a lot of technology at the reader, the authors break it down by its functionalities and support their premise with actual cases including Titan Rain. In Chapter 10, we see actual screenshots showing how criminal-oriented malware is used; the authors’ backgrounds in security companies has given them real-world experience. I really appreciated Chapter 11. How can they keep making malware we can’t detect? You will get to see the tools that are actually used.

Amazingly, the authors are able to pull it all together; Chapter 12 serves to focus what you have read. In fact, to get the most out of the book, you might want to start with Chapter 12 and read the MOSAIC framework section. MOSAIC is designed to help an analyst correctly evaluate cybercrime and cyber attack information. It stands for

- Motive awareness
- Open source intelligence collection
- Study
- Asymmetrical intelligence correlation
- Intelligence review and interrogation
- Confluence

Or, as the authors say in the summary, remember to focus on the three dimensions of _people, process and technology_ and your security efforts will be much improved. This book has lots of information on all three dimensions. It was a pleasure reading it and to develop this foreword, and I am sure you will find it advances your knowledge on cybercrime and espionage.

Stephen Northcutt

President, The SANS Technology Institute, a security graduate school
PREFACE

Thank you for picking up this book! We believe that if you are reading this page, you are an individual seeking to gain a greater degree of familiarity with cybercrime and espionage, and more likely than not, believe that the realities outweigh the fear, uncertainty, and doubt associated with these two topics. Our desire in writing this book was to initiate a conversation pertaining to the subject matter from a different perspective. Given that both of the authors have backgrounds with the Department of Defense (DoD), intelligence community, and the commercial information security industry, we felt it appropriate to begin asking tough questions while providing answers to nontrivial challenges. This is not a work of fiction. It is our belief that this book will aid in changing the perception of cybercrime and espionage by joining the ranks of books written on the topic while, at same time, approaching the subject matter with a fresh perspective. We set out to achieve a goal and believe that we have achieved the first of many milestones in total goal attainment. This book has proven to be challenging to write as it has challenged us to reconsider our beliefs, perspectives, opinions, and experiences and approach them and the project with an independent perspective. A great deal of work was spent corroborating facts and figures, as standard bodies for this area of study do not exist. Making matters more complex was the challenge of redefining “loss” with respect to our industry in addition to properly defining totals as they pertain to frequency of occurrence and dollars spent or made perpetuating events of interest the likes of which are discussed within this work. We believe that we are just scraping the tip of the iceberg with this book and have no doubts as to the need for further expansion and definition. We knew in beginning of this project that the volume of material to be discussed was great and that it would be difficult, to say the very least, to address every aspect (doing them justice) in gross detail in a single installment. As a result, we view this as a stepping-stone in our journey to explore this area of study in greater detail and assert that the journey has just begun.

Best regards,
Will Gragido and John Pirc
October 18, 2010
ACKNOWLEDGMENTS

Will Gragido

This book is a labor of love, devotion, and duty. I am privileged to have written it with my peer, colleague, and friend, John Pirc, a true cyber warrior whose dedication to his work, family, and friends knows no bounds. You are a warrior and a scholar; I hail your sense of balance and duty! I would also like to thank my friend, mentor, and boss, Mr. Greg Adams, whose support and guidance have been and continue to be invaluable; thank you Sir! I wish to extend special thanks to my lovely fiancée, Tracy Long, whose understanding, patience, and support were integral to me during the process of creating this book. Additionally, I would like to thank my children, Luz Maria and Ava Elizabeth; I love you both more than life itself and hope that the work we have begun in this book aids, even in some small way, your lives and the lives of your children going forward. I would also like to thank Mitchell, Jeremy, and Jameson Pogreba, my stepsons; I love you boys; you make me proud! And last but certainly not least, I would like to thank my mother and father, Mary Alice and William L. Gragido, for giving me life and welcoming me into the world to fulfill my destiny; I love you mom and dad.

John Pirc

I want to thank my Lord and Savior Jesus Christ as none of this would have been possible without my strong belief in Him. I am thankful for the opportunity to have coauthored this book with my great friend and colleague, Will Gragido. I cannot thank Will enough for all his efforts with this book and encouraging me to kick this ball over the finish line. Additionally, I want to thank my awesome wife, Lisa Pirc, who gave me the necessary time away from the family to complete this book. To my children, Kelsey, Aubrey, and Jack...thank you for your understanding while daddy was writing this book. I am very proud of all three of you! Lastly, I have to thank a few more people who have been instrumental in my personal life and career. John Lawrence, thank you for being there for me and covering my college tuition and encouragement to finish. Ed Willars, thank you taking me in like a son and sharing Christ with me! Greg Adams, thank you for the great example you have set both inside and outside of work and for allowing me time to finish this book...it has been and
continues to be a pleasure to work for you! Kris Lamb, Dan Holden, David Ostrowski, Jim Brennan, Munawar Hossain, John Trollinger, Charlie Stokes, David Dewey, Mike Dausin, Wayne Blackard, John Webster, Bob Bigman, Jerry McEvoy, Cedric Deal, Dave Farnham, John Viner, Randy Hulette, Nick Lantu, and Glenn Snow...thank you for investing your time in me! I cannot begin to tell you how thankful I am. To my best friend Eric York; you are like a brother to me and thank you for the encouragement while writing this book. Lastly, Mom, Dad, Jamie, Tonya, Lydia, Lara, and Dan, I love you and thank you for all that you have contributed to my life.
ABOUT THE AUTHORS

Will Gragido is a seasoned information security and risk management professional with over 15 years of professional industry experience. Will has deep expertise and knowledge in operations, analysis, management, professional services and consultancy, presales/architecture, and business development within the information security industry. Mr. Gragido holds the CISSP and CISA certifications, as well as accreditations in the National Security Agency’s Information Security Assessment Methodology (IAM) and Information Security Evaluation Methodology (IEM).

John Pirc has more than 10 years of hands-on security experience in security research, worldwide product management/development, security IV&V testing, forensics, and architecting/deploying enterprise wide security solutions for both public and private organizations worldwide. John was recently named security thought leader of SANS Institute and advisory board member of SANS Execubyes publication.