SYNGRESS

Cybercrime and Espionage

An Analysis of Subversive Multi-vector Threats

Will Gragido
John Pirc

CYBERCRIME AND ESPIONAGE

This page intentionally left blank

CYBERCRIME AND ESPIONAGE

An Analysis of Subversive Multivector Threats

WILL GRAGIDO
JOHN PIRC

RUSS ROGERS, Technical Editor

ELSEVIER

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

SYNGRESS®

Acquiring Editor: Angelina Ward
Development Editor: Heather Scherer
Project Manager: Andre Cuello
Designer: Alisa Andreola

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods 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
Application submitted

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

ISBN: 978-1-59749-613-1

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

For information on all Syngress publications
visit our website at www.syngress.com

CONTENTS

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 installatment. 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

This page intentionally left blank

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 Execubytes publication.

1

CYBERCRIME AND ESPIONAGE AND THE NEW SECURITY 101

INFORMATION IN THIS CHAPTER

- He Who Does Not Prevent a Crime When He Can, Encourages It
- What's Old Is New Again
- A Changing World
- Cybercriminal Statistics: U.S. and Abroad
- The Statistics of Cybercrime
- Separating the Wheat from the Chaff: Qualifying Amateurs and Professionals
- Trends in 2011
- Myopic to the Catastrophic: Advanced Persistent Threats
- Points of Confluence: Events That Have Shaped the Future of Privatized Cybercrime and Espionage
- Agendas in Next Generation Cybercriminal Activity
- The Coming Decade

Introduction

The Roman statesman Marcus Tullius Cicero (b. 106 B.C.–d. 43 B.C.) when speaking on the nature of criminality, once said that "The enemy is within the gates; it is with our own luxury, our own folly, our own criminality that we have to contend." Put another way, Cicero had clearly identified what he believed to be the root cause for much of what ails all humanity. Cicero believed that the enemy—or the threat that comprised it—had already breached man's defenses as a race. Perhaps, it had compromised the perimeter defenses of early man long before Cicero's time and had firmly taken root in the ecosystem of mankind's very existence. He clearly states that it is man's desire toward luxury (in Cicero's days, just as in our own, the desire for

luxury was ubiquitous and the means by which some sought to achieve and maintain it were, just as they are today, less than honorable and often exploitative in the best of cases), his willingness to commit folly (his willingness to participate in, orchestrate, and execute idiocy or madness), and his criminality (which just as in Cicero's day is today a direct result of our lack of ethics, morality, and a galvanized sense of right and wrong) that must be recognized, managed, and mastered. Failure to do so only encourages the proliferation of the behavior and the aftermath that it yields. Cicero knew this to be the case and was cautioning future generations to take heed of what was occurring within his world because if it could happen in Rome, it could, and would, happen anywhere. Cicero was a very wise man.

This quote with respect to the nature of criminality has, since the first time the authors encountered it, struck them as being both insightful and profound. Cicero had articulated in a ubiquitous manner the nature of those who willingly partake in criminal acts. Cicero's point is simple and warrants reiteration. For Cicero, humanity (regardless of how simple or complex the society) owns its criminality and its propensity toward it.

He Who Does Not Prevent a Crime When He Can, Encourages It

Seneca, the Roman philosopher (first century A.D.), once said "He who does not prevent a crime when he can, encourages it." In Seneca's view inaction equated to action that ultimately encouraged (when speaking about crime) the perpetuation of criminal activity. Actions are ultimately influenced by a number of variables—some much more within the boundaries of our immediate control than others. Some are fed and fueled by our ethics and morality while others are influenced by a lack thereof. Regardless crime is, as Cicero asserts, an enemy that warrants immediate attention and the battle begins within each one of us. Criminality in all its forms ultimately comes back to man's interpretation of law and governance and what is or is not perceived as being allowable in relation to the accepted norms set forth by law. At a primitive level, it is an extension of the struggle between that which is deemed "good" and that which is deemed "evil." It is a terrifically powerful idea to grasp—one that forces each of us to conceptualize our own proximity to "good" and "evil" and to "right" and "wrong" while considering the idea itself with respect to its universal

implications. It is an idea that transcends time and one which future generations (just as those that have come before them) will struggle against. Though this may sound inconceivable, we must bear in mind that not all is lost and that just as Cicero pointed out, the enemy is and always has been within the gates, and also that where there is life there exists hope. It is this idea that we will strive to explore, flesh out, and extol throughout the entirety of this work.

Criminal activity is a reality of the world in which we live. So too is espionage and often the two are not mutually exclusive. This is not a new concept. It is however a reccurring theme which bears repeating. One question we are often asked is whether there is any hope in combating this activity. People are curious as to whether this is possible either in the traditional sense or in those areas in which there has been a unique evolution such as that within cyberspace and the Internet—and the answer is yes, there is hope; however, it comes at a price. Moreover, it is not a trivial undertaking and should not be presented in a light that either under-emphasizes or over-aggrandizes it.

Our attitudes and approach to these challenges must evolve as well and like Cicero, we must recognize first that the enemy lies within before we begin to master those who threaten us from external vantage points. We must steel ourselves in the knowledge that we must cultivate and develop a sense of vigilance that lends itself to the development and proliferation of those who seek to combat the actions of the criminally inclined. In doing so, we encourage and enable ourselves to detect, identify, and prevent criminal activity and gain a greater degree of insight into the psychological motivations and drivers at work within these individuals and groups while enabling a more robust understanding of the tactics, strategies, and plans being executed on a global basis to accomplish their means. Never before has the world been more ripe for the taking by sophisticated entities bent on profiting at all costs, in defiance of local and international law, let alone socially accepted definitions of normative behavior associated with ethics and morality. As a result, a new breed of information security professionals must be armed and equipped with the tools necessary for addressing these adversaries and their actions.

What's Old Is New Again

At this point in the chapter, you may be wondering just why we are discussing the philosophical aspects associated with criminality in a book dedicated to cybercrime and espionage.

It is a valid question and one that requires an equally valid response. To begin with, as we have established, humanity is its own greatest threat. This is likely not a huge shock to you, the reader, if you have read any philosophy in school or turned on the evening news. However, it is important that we stress this point as it is the basis for understanding much (if not all) of what influences criminal activity. In many respects, the same root influencers are present when speaking about traditional criminal activity or next generation criminality such as that which is most often associated with cybercrime and espionage. As a result, we must diligently work to mitigate the risks associated with those behaviors, which fall into categories defined as being criminal and deviant from the norm. Equally important is our understanding that engaging in criminal activity is a choice. It is not something that just happens, though there are rare occasions when this is the case.

Throughout recorded history, human beings have achieved incredible milestones, demonstrating the superiority of our species in both evolving and adapting to our changing environment. We see this in every aspect of our world and it should come as no surprise that we excel in subverting laws and governance with the same ease and elegance as in other areas in which we continue to push the envelope of achievement. Examples of human determination and drive can be cited all the way back to the Neolithic era (roughly 10,000 years ago), when man matured from hunter-gatherer to farmer. As our societal trends and patterns continued to evolve and grow along with our natural migratory patterns, so did our technological advances. Crude implements gave way to more consistently designed and manufactured tools. Techniques and ideologies were developed to aid in ensuring bounty. While these aspects of humanity flourished (to its credit), so too did its challenges, in particular those dealing with morality, good, and evil in the eyes of the law as it existed at that time.

Evidence that this struggle existed long ago can be seen in the ancient Chaldean/Babylonian text, the Code of Hammurabi (ca. 1750 B.C.). This work, also known as the Codex Hammurabi, has some 282 laws, some with scaled degrees of severity, depending on a person's social station. Some examples of the Code of Hammurabi are given here:

- If anyone ensnares another, putting a ban upon him, but cannot prove it, then he that ensnared him shall be put to death.
- If anyone brings an accusation against a man and the accused goes to the river and leaps into it and sinks, then

his accuser shall take possession of his house. However, if the river proves that the accused is not guilty, and he escapes unhurt, then he who had brought the accusation shall be put to death, while he who leaped into the river shall take possession of the house that had belonged to his accuser.

- If anyone brings an accusation of any crime before the elders and does not prove what he has charged, he shall, if a capital offense is charged, be put to death.
- If a builder builds a house for someone, and does not construct it properly, and the house that he built falls in and kills its owner, then the builder shall be put to death. (Another variant of this is that if the owner's son dies, then the builder's son shall be put to death.)
- If a son strikes his father, his hands shall be hewn off.
- If a man gives his child to a nurse and the child dies in her hands, but the nurse unbeknown to the father and mother nurses another child, then they shall convict her of having nursed another child without the knowledge of the father and mother and her breasts shall be cut off.
- If anyone steals the minor son of another, he shall be put to death.
- If a man takes a woman as his wife but has no intercourse with her, then this woman is no wife to him.
- If a man strikes a pregnant woman, thereby causing her to miscarry and die, then the assailant's daughter shall be put to death.
- If a man puts out the eye of an equal, his eye shall be put out.
- If a man knocks the teeth out of another man, his own teeth will be knocked out.
- If anyone strikes the body of a man higher in rank than he, he shall receive 60 blows with an ox-whip in public.
- If a freeborn man strikes the body of another freeborn man of equal rank, he shall pay one gold mina (an amount of money).
- If a slave strikes the body of a freed man, his ear shall be cut off.
- If anyone commits a robbery and is caught, he shall be put to death.
- If anyone opens his ditches to water his crop, but is careless, and the water floods his neighbor's field, he shall pay his neighbor corn for his loss.
- If a judge tries a case, reaches a decision, and presents his judgment in writing, and it is later discovered that his decision was in error, and that it was his own fault, then he shall

pay 12 times the fine set by him in the case and be removed from the judge's bench.
- If during an unsuccessful operation a patient dies, the arm of the surgeon must be cut off.

As one can see, many of these laws were, for the time, quite relevant and arguably necessary in maintaining order in a world that was continuing to evolve though we would today frown on and discourage roughly 99% of them from a twenty-first century perspective, some of them are almost absurd, while it could be argued that others are still relevant. There are limitless examples that can be cited from the ancient times the world over, which underscore two key points: criminal behavior is neither new nor is it something to be taken lightly. As a result, developing the ability to swiftly and accurately detect criminal activity as it morphs is of paramount importance to those tasked with defending against it and sitting in judgment of the accused when the time comes to do so. Equally important is the ability for those tasked with preventing criminal activity to realize that regardless of the form in which it manifests, behaviorally it is neither new nor original.

Certain elements and factors will remain prevalent in the exploration and expansion of criminal enterprise, namely, the risk-to-reward proposition. It is for this reason that the authors and other leading researchers and analysts who devote their time and energy to studying the behavioral patterns and activities of criminal actors believe that the rise in cybercrime has increased dramatically on a global basis. As we shall see throughout the remainder of this book, the evolution revolution within the criminal underworld is squarely upon us and has been so for some time. As King Solomon once said, "What has been will be again, what has been done will be done again; there is nothing new under the sun" (Ecclesiastes 1:9, New International Version). Though debates rage within theological circles regarding the authenticity of the book (Ecclesiastes) and its attribution (authorship traditionally attributed to Solomon, King of Israel), few question the honesty and ubiquity of its message, its timelessness, and the fact that it transcends arguments related to the validity of religion and faith. The message is clear: things tend to be cyclical, and to a degree, predictable in their individual and collective states of unpredictability. Nowhere is this more the case than in the realm of information security, specifically when addressing the rise of cybercriminal activity and espionage in the twenty-first century.

A Changing World

Over the course of the last two decades, the world has become more connected than ever before. The importance of geographic disparity has become an outdated concern. It has become outdated, as distance has, in effect, died. This is largely due to the rise and viral expansion of modern data and telecommunications networks, and of course, the intoxicating allure of the Internet and World Wide Web. Never before has humanity experienced this level or degree of interconnectivity. Our collective perspective has forever been changed and there is no turning back. We are simply in too deep to consider extrication from today's technologically infused world. To assert the contrary is akin to seeking disconnection from the human race itself. At this point in human history, it is virtually impossible, given the interdependencies and complexities associated with such a task. Our lives, our work, our ambitions, our entertainment, our finances, and our identities, like it or not, are interwoven in a web of 1s and 0s, which exist in a virtual plane of our creation.

With a click of a mouse or touch of a Smartphone screen, distances that in the not so distant past were thought to be insurmountable, are conquered in milliseconds. This degree of reach has enabled the achievement of dreams on a scale previously undefined. Collaboration, leading to advancements in technology, science, biomedical research, the arts, finance, and commerce, has become a reality that in the past would have been thought impossible. An unforeseen byproduct of these revolutionary advents has been the increased potential for criminal activity and exploitation previously unconsidered. The attack surfaces that what we individually and collectively possess, as Cicero points out, have grown, while society and its members, as Seneca suggested so long ago, are faced with decisions regarding activity or inactivity in addressing and preventing criminal acts.

Whether we wish to admit it or not, our advancement has in fact increased our risk posture, increasing our susceptibility to exploitation and compromise forever. Like Pandora, who unleashed upon the world great evils and ills after opening her jar, we too find that hope still exists and persists if we choose to see it. However, to be able to consider hope we must first equip ourselves for battle. We must ready ourselves for the advances of enemies seen and unseen. We must educate others and ourselves so that we are prepared for any challenge that we might face, thus minimizing our exposure to risk and adversaries.

Cybercriminal Statistics: U.S. and Abroad

"Figures don't lie; but liars figure."

–Samuel Clemens a.k.a. Mark Twain

Assessing in a consistent quantitative manner the actual numbers associated with total potential revenues, real revenues, and loss associated with cybercriminal activity and espionage is a nontrivial task. As we shall see in the coming chapters, it is difficult to denote (with total accuracy) the numbers associated with both profit and loss, largely because those who have been exploited (whether via a credit card scamming event, a fraudulent email attack, or an example of corporate or state-sponsored espionage) are often times very reluctant to come forward to authorities. Depending on the nature of the attack, the scale, sophistication, and whether or not the victim realizes he or she has been compromised—especially in the case of corporations and governments—decisions regarding whether or not to disclose are often arrived at after calculating the single loss expectancy and annualized loss expectancy associated with the event of interest. Many times the results arrived at from these calculations are looked at in concert with other salient data points having to do with branding, valuation, positioning, global financial positions, and so on.

As a result, efforts to amass meaningful statistical data for the purpose of analysis are also nontrivial. Speculation and debate about what is *real* and what is *fiction* rage on. Sources, some credible, some of less sound repute, must be verified along with disparate data sets in the hope of arriving at a place of clarity with respect to these numbers. Variables of both quantitative and qualitative origins must be weighed alongside more traditional information that at times looks at the qualitative, calling into question the authenticity, motive, and accuracy of the quantitative.

Note

The celebrated American humorist and author Mark Twain once had this to say about statistics, "Figures don't lie, but liars figure." Twain, who was suspicious of statisticians, among others, provides an important insight for us: numbers are simply numbers and are dependent on those who calculate, collect, analyze, and disseminate them to be represented and weighed accurately. The authors of this book agree with Twain and because of this have endeavored to represent all statistical information in the most pure and accurate form and fashion possible.