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.

When discussing statistical data associated with cybercriminal activity, there are many points to consider, the most salient being a natural extension of traditional criminal activity and by proxy a natural outcropping for organized criminal entities of various denominations. Though it is not without risk, the risk is far less evident than in traditional forms of criminal activity and behavior, and the instances, which the mass media are aware of, represent a subset of the activity actually occurring in real-time the world over. The authors believe that in assessing data sets associated with cybercrime and espionage, many parties would prefer that empirical evidences remain vague, allowing them to offset and arguably downplay the existence and impact of such activity on the world around them.

The reality is that the numbers associated with activity of this sort (which will be defined in more granular detail later on) are truly staggering. They continue to grow at a rate of growth which some, including the authors, feel are of epidemic proportions. As this is the case, the importance of collecting and excogitating as much data as possible remains of primary importance in conducting a proper analysis. No work of this type would be worth the paper it is printed on without the proper degrees of due diligence being performed. This must occur in order that we individually and collectively avoid the pitfalls associated with underestimating the realities of such activity while carefully avoiding the equally perilous mistake of exaggerating them, thereby ushering in an irresponsible level of fear, uncertainty, and doubt. A key goal and outcome of this book is, among other things, to see the creation of a definitive source or body whose charter is to monitor such activity globally, taking into consideration trends in localized geographies as well as those which manifest in multiple geographic theaters. In doing so, security researchers and professionals as well as law enforcement, academic, and various government and military institutions will be positioned to assemble clear, concise actionable data yielding a greater degree of understanding and comprehension.

The Statistics of Cybercrime

Much can be said on the importance of accurate statistical information. In fact, entire books are written with respect to this subject, yet there is no definitive source dedicated to the topic of cybercriminal statistics. Perhaps, because of the lack of a definitive body of knowledge with respect to cybercriminal statistics, it is no small wonder that there is a misconception in the world today surrounding the frequency, rate, and history of this type

of activity. Electronic, computer-based, and Internet crimes are not new. It is an extension (and a logical one) of traditional criminal activity being executed by either criminal professionals or amateurs endeavoring to reap profits. Organizations such as the Internet Crime Complaint Center (IC3), a partnership developed between the United States Federal Bureau of Investigations (FBI) and the National White Collar Crime Center (NW3C), which began its work in May 2000, release annual reports which account for statistical information related to reported complaints.

The IC3's mission is to address crimes committed over the Internet that are reported to it. It accomplishes its mission by facilitating the flow of information between law enforcement agencies and the victims of fraud, crime, and information that may otherwise go unreported. The IC3 released its annual report for the calendar year 2009 on March 12, 2010. In it, the organization focused on fraudulent activity being conducted within the Internet and cyberspace. The report accounts for the fact that complaints of crimes committed online were up substantially from the previous year. In fact, the report suggests that there was an increase of 22.3% from 2008 to 2009, which yielded a gross increase of 294.7 million USD. This increase brought the total number of known losses in the United States to 559.7 million USD, a staggering figure by any account, yet one that is met with much controversy as it is seen as a conservative assessment of the totals associated with loss due to this activity. Some of the more salient details are represented graphically in Figure 1.1.

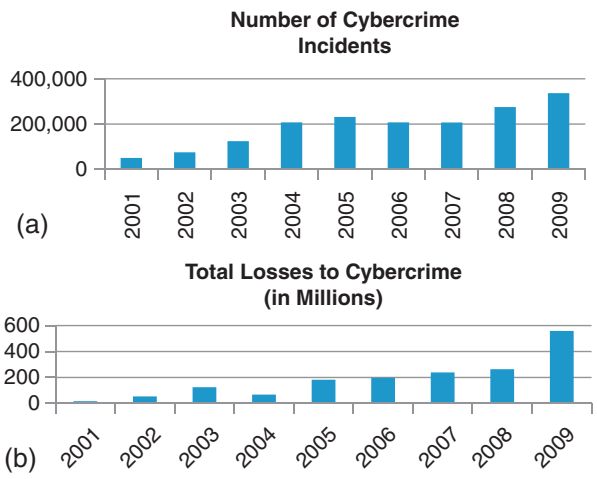


Figure 1.1 (a) Number of cybercrime incidents. (b) Total losses to cybercrime (in millions).

Separating the Wheat from the Chaff: Qualifying Amateurs and Professionals

On taking into account all that has been discussed so far, a few logical questions rise to the surface. First, who are the people responsible for this activity and what is their motive? Second, do we have any real insight into their numbers? What are their intentions and motivations? Are they largely amateurs or are there as many professionals

involved as we are led to believe by the media? These are not easy questions to answer; however, as we will see throughout this book, many, if not all, of these questions will come up again and hopefully be answered in the most detailed manner possible. Criminals come in all shapes and sizes; all races, creeds, and religions. They operate within all levels of society, at varying levels of sophistication from the truly banal and amateurish to the fiercely guarded, structured professional organizations which from time to time make the news and are central figures in some of Hollywood's most entertaining blockbusters. Criminals by definition are those who willingly participate in acts that qualify as deviant behavior in the eyes of society and the law. This behavior violates the norms of society and its culture. It defies the standards by which people live and operate within a society, challenging any to take action if they dare.

As a result, the people who are responsible for this activity could be sitting next to you at a restaurant or bar, on an airplane, or in a theater. The ultimate motivator for all who endeavor to act criminally in the context in which we are working is to net a profit via the exploitation of others (individuals, businesses, governments, etc.), while incurring the least amount of risk or harm.

As we will discuss in later chapters, the levels of sophistication and skill set have changed dramatically over the last 20+ years. Though many factors influence this, the following represent some of the more commonly recognized ones:

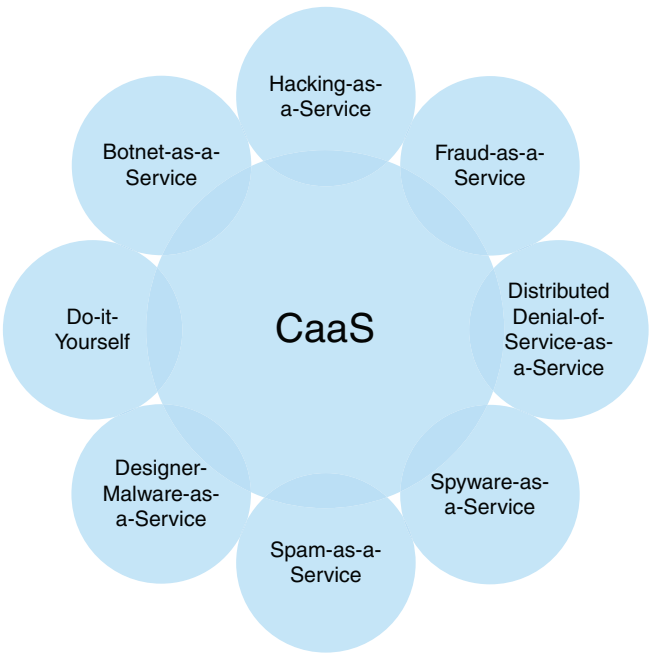
- The disintegration of nation states and the modes of operation which were employed by those states (politically, economically, militarily)
- The rise of interest and expansion by traditional criminal organizations the world over in electronic criminal activity, fraud, and cybercrime
- The availability of data and telecommunications technology
- The overwhelming availability of materials and knowledge transfer making it easier than ever before to compromise a system for profit
- The potential to profit in ways which were previously relegated to works of fiction writers

As we shall see, those cyber actors who actively participate in activity of this sort range from the "newbie" to the "seasoned" professional and represent all lifestyles. Paradigms which were of crucial importance in the yester year of cybercrime, most notably that of notoriety, are now deemed a sign of the amateur although there are cases where it is devilishly difficult to deduce whether what we are seeing is the work of an amateur because of the way in which it was executed or if it was part of more

sophisticated, cleverly crafted plan and strategy executed by professionals working in a criminal or state capacity. Nevertheless, the field of battle has changed forever and so too have the actors that stride on it. Today's world sees profit being the primary driver (again due to the lower risk factors), while motivators such as politics, philosophy and theology, and to a lesser extent activism, come into play from time to time. The net result however is that a new breed of cyber actor is upon us and as we shall see, acts at times individually while at other times very much in collusion. In addition, just as there are new actors emerging within the ecosystems being driven by criminally motivated activity, so are we seeing new consumers of the goods and services provided by these actors. In Figure 1.2, we present a high-level view of some, *not all*, of the types of services that are provided today by cybercriminals for profit.

As one may guess this is simply the tip of the iceberg and as we gain clarity into the realms of the cybercriminal world and the deep web, we will most assuredly be able to (with greater degrees of accuracy and proficiency) identify and define new and growing criminal services. Although geolocation is important, it is equally if not more important to recognize that localization exists and extends to the hearts, minds, and legislature of the nation states in which many cyber actors actively pursue their trade craft. Put another way, in many nations (we will see this in later chapters), identifying the existence of a cybercriminal enterprise in a given nation state does not equate to it being illegal.

Figure 1.2 Crimeware as a service.



In many cases, legality is in the eye of the beholder. Already this has proved to be a sticking point in many cases being pulled together and processed in the United States and will no doubt continue to be the trend in the foreseeable future. Nevertheless, subeconomic ecosystems have emerged the world over, offering a wide variety of products and services such as those represented in Figure 1.2 with unparalleled profitability in sight.

Trends in 2011

In 2010, Facebook surpassed Google for total number of hits and page searches. It was the first time a social networking solution had surpassed a search engine in any capacity in the history of the Internet. It marked the dawn of a new era, an era that could no longer be ignored, dismissed, or looked on as a fad. The age of social networking had arrived in full force and was here to stay. Social networking sites along with other Web 2.0 technologies have become ubiquitous elements of our world. As household names, they are present and accounted for within our professional and private lives, infiltrating our hearts and minds while offering the opportunity to connect or reconnect with one another like never before. Who does not love the opportunity to reconnect with old friends, to see pictures of Aunt Sally's vacation to Bermuda, or join a group dedicated to their favorite sporting team while tending their crops in a video game dedicated to, you guessed it, cyberfarming?

Social networks associated with modern computing and communications have penetrated the social fabric. They have changed forever the etiquette associated with acceptable use and disclosure at the workplace and at home. They have made it both plausible and possible to blurt out an entire thought in 140 characters or less. Their importance has been etched into the cultural zeitgeist and as we bore witness to their emergence and growth, so too do we bear witness to their ability to inextricably impregnate themselves within modern society. The illusion of inextricability had been cast and there was now seemingly no room for a world without them. In 2010, there is no question that Facebook is the most popular of all social networking or media sites. It has revolutionized the space through the elegance achieved via its simplicity. But at what cost? Though not the first of its kind, Facebook has redefined the market space in which it was launched after having been conceived and launched by cofounders Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes while attending Harvard University. With help from industrious venture capitalists, Facebook will swiftly leave its predecessors in Internet obscurity.

Social networking media sites and Web 2.0 architectures continue to flourish and grow. In addition to their explosive growth, they have become bastions for malicious code and content propagating and perpetuating the said code via a variety of infection vectors. They proliferate with new offspring and features such as mobility, surveys, and games, for example, at a pace that would have caused the most forward-thinking minds of the last

century to note. Their advancement, as we have noted, has had a profound impact on our world in ways which were previously unimaginable. Although social networking and media sites are considered an increasingly important part of normal life, they are not without their downsides.

These sites have become targets of opportunity for cyber actors of all denominations, many of whom have nefarious criminal intentions. As a result, compromising and exploiting unsuspecting users have continued to rise via social engineering attacks and the propagation of malicious code and content. So prevalent are the attacks that one of the authors of this book had a cousin whose email and Facebook account were compromised by a Canadian high-school student via a poisoned URL attack executed via a Farmville invitation. These threat vectors, and many others, have led to innumerable compromised hosts (such as the author's cousin) along with countless weakened corporate and personal risk postures. Estimates of loss associated with these compromises vary and in some respects are truly impossible to calculate. Compromises related to social networking technologies have proved to be particularly challenging to properly assess because of the role that geographic localization plays today in relation to malicious code and content.

Via Web 2.0 technology, these sites offer end users (legitimate and illegitimate) the ability to craft customized sites within a given language and dialect reflecting that which is relevant geographically in addition to that which is relevant on a global basis. This new advent in localization has proved to be a great challenge to those tasked with combating new and exotic threats as they deviate from the familiar, a fact being counted on by our adversaries. In years past, localization simply referred to geographic location associated with a given type of malicious code or content. Via advances in internetworking and our ever increasingly interconnected world, the paradigm has shifted and thus the inclusion of this new localization.

However, 2010's threats were not limited to the realm of the social network. Pandemic-like rises in both appearance and documented infections were noted with respect to new and much more mature threats than had ever been seen before. Advanced command and control (C&C) driven bot-networks continued to ravage the Internet landscape, compromising hosts the world over and earning their owners profits that would rival, if not surpass, many legitimate business endeavors. These bot-networks, and their owner-operators (as well as their clientele) represent a truly diverse portrait of those responsible for the generation, propagation, marketing, and sale of advanced malicious code.

Although not a new technological threat (in fact theirs is a well-established pedigree dating back to the late 1990s with voluminous amounts of data—formal and informal, academic and practical—to support their existence, architecture, and use), bot-networks continue to prove effective means of disseminating malicious code and content not to mention terribly effective architectures for the harvesting of data from targets of interest. They are challenging and proven adversaries the likes of which most information security agencies, regardless of their level of experience or years in industry, have encountered.

Consequently, the bot-networks or "botnets" have become increasingly more popular among amateurs and seasoned professional cybercriminals alike. They offer the newbie an easy entry point into the murky depths of the subeconomic ecosystems emerging within cyberspace, while at the same time continuing to provide lucrative profits for their masters. Botnets such as Blazebot, Monkif, Clampi, and ZeuS, in addition to the now infamous Storm-bot (also known as Waldec), have all made their appearance in 2010, surging through the Internet and enterprises the world over without mercy. These threats often lay dormant within unsuspecting systems and environments awaiting commands from their botmasters, ready, willing, and able to carry out the directives they receive. Technologies such as cloud computing have proved to be a fertile haven for this type of activity and, as a result, have unwittingly undermined the value propositions their architects and pundants work so diligently to espouse.

An example of this occurred in 2009. Security researchers at Computer Associates discovered that a ZeuS bot-network (a password-stealing bot-network noted for its involvement in excess of 100 million USD) C&C server was found hosted and operating within Amazon's Elastic Computing Cloud (EC2),[1] an environment previously touted as being impregnable and safe for secure business and personal transactions. Though speculation

[1] *www.securityfocus.com/brief/1046*
http://news.cnet.com/8301–1009_3–10413951–83.html
http://aws.amazon.com/security/zeus-botnet-controller/
www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/
http://community.ca.com/blogs/securityadvisor/archive/2009/12/09/zeus-in-the-cloud.aspx
http://news.techworld.com/security/3208467/botnet-found-in-amazons-ec2-cloud/?intcmp=ft-mdb-rtd
www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110
www.pcworld.com/businesscenter/article/184159/hackers_find_a_home_in_amazons_ec2_cloud.html

ensued with respect to the EC2 being a target of choice or a target of opportunity, what could not be disputed was that it had been compromised by one of the world's most sophisticated and successfully evolving bot-networks while also proving again that no environment is beyond reproach. Malicious code and content numbers have experienced a surge unlike at any time previously. Current estimates suggest that since 1983, more than 40 million individual samples of malicious code and content have been detected, identified, and observed in the wild, with nearly 30 million of those samples being accounted for in 2009. Research suggests that this number will continue to rise and it should be noted that security researchers the world over are concerned with the volume and quality of samples being collected. Additionally, researchers struggle with what *is likely escaping their notice*. This concern is warranted as statistics suggest that commercial cybercrime and espionage are on the rise, which further suggests that demand will be met with supply. At the time of writing this book, new and innovative threats have emerged and in some cases reemerged as examples of activity that further supports the claims being made by security researchers, law enforcement, the military, the intelligence community, and the authors—criminal activity associated with "cyberspace" is increasing. As our dependency on Internet-based services and applications deepens, so too does our susceptibility to exploitation.

Other technologies such as virtualization platforms have also become increasingly more popular within privatized business as well as the public sector, from Wall Street to Waltham, Massachusetts. Though quite innovative and compelling from an ROI (return on investment) and TCO (total cost of ownership) perspective, these platforms have proved problematic from an information security perspective and continue to represent concern with respect to compromise and exploitation. Evidence suggests that sophisticated cybercriminals have begun developing techniques for manipulation and application of advanced routing protocols such as IPV6 to prepare the way for the next generation of exploitation, while more traditional fraudulent activities such as poisoned URLs or look-alike URLs maintain strong use due to their effectiveness.

Myopic to the Catastrophic: Advanced Persistent Threats

In 2010, a new acronym has come into vogue, which has befuddled, perplexed, confused, and at times, unnecessarily

muddied the ever murky waters of the information security industry. That acronym is APT or Advanced Persistent Threat. Incidents involving Google, Inc.'s efforts in China and "Operation Aurora" seemed to propel the term into the forefront of all things information-security related. A great deal of misinformation and confusion was caused by this and as a result the term began being adopted and bastardized by marketing campaigns bent on convincing consumers that the widget of choice had guaranteed efficacy on Advanced Persistent Threats. This of course was but is not the case. There is no silver bullet, as we shall discuss in later chapters, for Advanced Persistent Threats or more advanced taxonomic families such as Subversive Multivector Threats.

Advanced Persistent Threats have traditionally been seen in the defense intelligence base, the Department of Defense, and within the Intelligence community; however, there have always been exceptions to these unwritten rules. The purpose behind threats of this sort is to remain hidden, acting in a clandestine manner to gain and retain continual, unfettered persistent intelligence observation on individuals or groups of individuals. Within the information security industry, the term is most often used to specifically refer to a subset of threats typically seen associated with long term, targeted attacks where nation states, corporations (DIB, Biomedical Research, High Tech Research, etc.), and political figures (e.g., the Dalai Lama) are the targets.

Research, in addition to historical record, suggests that all modern or advanced nation states have employed and continue to employ some form of these threats. This should come as no surprise, given the nature of most of these compromises and attacks and the way in which they are used to siphon data in voluminous quantities. Definitions of precisely what an APT is can and often do vary; however, they can largely be summarized by the requirements defined by Beitlich:

- *Advanced*—Operators behind the threat utilize the full spectrum of intelligence gathering techniques. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence gathering techniques such as telephone interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly "advanced" (e.g., malware components generated from commonly available DIY—Do It Your self—construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple

attack methodologies and tools in order to reach and compromise their target.

- *Persistent*—Operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful.
- *Threat*—It means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The operators have a specific objective and are skilled, motivated, organized, and well-funded.

Points of Confluence: Events That Have Shaped the Future of Privatized Cybercrime and Espionage

As discussed previously, several factors influence and encourage both the participants and activity associated with cybercrime and espionage. Profiteering eclipses almost all others and although there are other notable reasons, profit remains at the forefront. Motivators and agendas vary however and as a result so too does the history that has influenced and continues to encourage its proliferation. Figure 1.3 provides a high-level

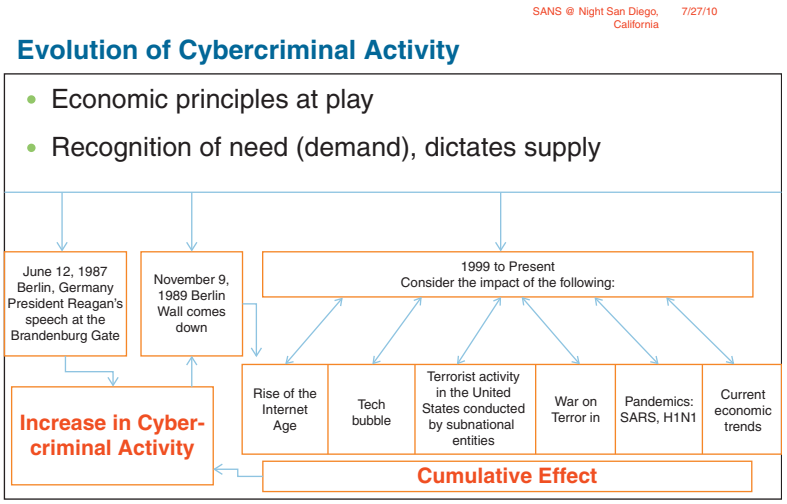


Figure 1.3 An evolution of cybercrime and espionage for profit.

insight into the rise of this activity on a global basis. It can be argued that the prevalence and availability of systems technology, educational materials, and global connectivity to the Internet and World Wide Web, along with the recognition of risk/reward factors by individuals, cooperatives, syndicates, organized crime entities, and subnational entities, are all equally important in the evolution of this activity and remain so.

Agendas in Next Generation Cybercriminal Activity

Agendas drive everything. This simple statement speaks volumes when taken in the context of our topic. Agendas provide structure and order to what would otherwise be nameless, shapeless, formless criminal activity. They provide direction and direction is of paramount importance to cybercriminals, amateur or professional, as it enables them to establish, define, and declare their primary motive: to achieve profitability while avoiding prosecution in any of its forms. Agendas are in essence nothing more than plans. Plans properly architected and defined enable the draftsman to execute them in a fashion that is meticulous and potent. As information security professionals of the next generation who have been chartered to aid in defeating such cyber actors, we must be prepared to recognize the relationship of agendas to both the tactical and strategic plans of our adversaries.

The Coming Decade

The next decade promises to be more dramatic than the last in terms of cybercriminal and espionage-based activity. The numbers of cases being reported to the United States Department of Justice show no signs of slowing and some of those prosecuted (e.g., the Alberto Gonzalez Operation) were directly responsible for some of the largest and most egregious acts of thievery in the history of the Internet. That having been said, cases of espionage are on the rise as well. We see inadvertent as well as deliberately architected operations occurring on a global basis such as Ghost Net and the more recent events surrounding United States Army Specialist Bradley Manning, currently being held in custody for what appears to be perhaps the most serious case of espionage and treason in recorded U.S. history with more than 260,000 classified documents having

been stolen and disclosed to the online whistle-blowing site, WikiLeaks. Whether these are outliers or direct indicators of what more is to come, the next decade demands that we must be vigilant and prepared for what lies ahead even in the absence of clear information.

Summary

In this chapter, we have introduced many concepts, some new and some old, but none of these should come as a surprise to anyone actively involved in or investigating for the first time the phenomena of subversive multivector threats. We have explored historical data as well as ideas related to trends and the idea that what is old will become new again. We see this frequently and there is no data that suggests that this trend will not continue. Additionally, we have explored statistical data related to cybercrime and noted the disparity and lack of correlation seen in these data sets universally. It is the opinion of the authors that this trend will need to change and that a standardized model and framework will need to emerge that dictate clear statistics and empirical data sets that outline events of interests, their trends, losses, and capital expenditure related to the perpetuation and mitigation of these threats.