Viruses and the Law

William M. Moss, Jr.

william.moss@knights.ucf.edu

Student, Masters of Science in Digital Forensics

University of Central Florida

Abstract

Viruses are a computer epidemic of epic proportions. This research paper provides an informative look at viruses from both a technical and policy standpoint. The work begins with a technical overview of viruses, their attack mechanisms, and a brief history of some of the most well-known offenders. Afterwards, three distinct arguments for policy framing are presented, focusing on traditional theories, an argument against traditional theory, and an innovative approach. These arguments are then discussed further and a potential framework is explored based upon the strengths and weaknesses of all three.

Introduction

Computer viruses, malware, and cybercrime have become a hot topic in technical and legal fields alike. Defending against network intrusions and cyber attacks has become critical across all levels of society at individual, corporate, and federal levels. This comes as no surprise, since information released by IC3 (2010) shows that losses reported to the organization in 2009 totaled $559.7 million, an increase of $295.1 million over 2008.

Viruses, the main topic of this paper, are a common method of perpetrating cybercrime. There are a broad range of effects caused by viruses, and the repercussions of a virus infection can range from miniscule to devastating. To fully understand the growing threat that this area of cybercrime poses to individuals, industry, and even national defense, one must first start with a technical understanding of how viruses *work*. From there, one may build upon what he/she knows, examining current theories on deterrence of virus writers as well as the effectiveness of current federal and state laws surrounding this area of cybercrime.

This is the approach that will be used in examining the issue of viruses and virus related laws. The second section will examine the technical side of viruses, famous viruses of the past and present, and significant court cases surrounding viruses and their writers. The third section will examine literature published addressing theories on computer crime, virus writers, and criminal prosecution. The fourth section will discuss the theories presented previously in greater depth, comparing them to what is known about viruses at present. Finally, the last section will summarize the findings of this work and draw conclusions about what is uncovered.

Technical Overview and Background

A Technical Overview

During the earlier days of viruses and virus detection, viruses were often strictly classified by the way they operated. Guinier (1991) and Kurzban (1989) both took care to clearly define the difference between viruses (which could infect a program but could not survive on its own) from other pieces of malware. Other malware types the two defined are worms (which are self sufficient self-replicating programs) and logic bombs (malicious pieces of code that had some sort of effect when a certain condition was true - such as the arrival of a specific date), among others.

Today, viruses are defined a little more loosely. Microsoft (2006) defines viruses as “small software programs that are designed to spread from one computer to another and to interfere with computer operation.” This broad ranging definition is likely due to the fact that today a virus may infect, operate on, and harm a computer in a variety of ways and may resemble one or more of the definitions presented by Guinier and Kurzban.

The term *virus* is often used by those who are less computer savvy to also refer to adware/spyware. Spyware programs, however, are programs bundled with other software that collect data from a user in order to advertise other products to the consumer. (SpyChecker, 2009) While this may be harmful and impact system performance, this type of malware is different from a virus due to the fact that it does not contain a mechanism for replication. This feature of viruses makes them extremely dangerous to computers and networks alike.

There are a variety of ways in which a virus can infect a computer or network and replicate itself. Guinier (1991) classified these mechanisms in two categories: internal and external propagation. According to the author, external propagation occurs at a level outside the computer (such as through infected diskette trading, message boards, or malicious sabotage by insiders, for example) while internal propagation happened entirely inside the computer after the machine had been externally infected. According to Guinier, internal infection occurrs when a malicious code piece attached to a program passes itself on to another uninfected program.

However, as technology has progressed, so have virus propagation techniques. Jiang, Li, and Zou (2009) introduce three distinct infection mechanisms. These are Web Download; Mail Attachment; and Automatic Scan, Exploit, and Compromise.

Web Download attacks occur when a victim machine downloads a small piece of malware when browsing the internet. Mavrommatis, Provos, Rajab, and Monrose (2008) present several ways in which this occurs. One of the most popular methods is through injection into a website (either by hacking the server and injecting it into the site, or by creating landing pages that redirect to the website after delivering the malicious code) via 0-pixel iFrames that are invisible to the naked eye and contain malicious code. (Mavrommatis, et al, 2008) The authors coin the name *drive by download* for this type of infection mechanism. Once the download has completed, the computers are connected to a network of other infected computers (known as a botnet) that uploads additional malware and updates. (Mavrommatis, et al, 2008)

Jiang, et al, (2009) describe email attachment infections as occurring most often through mass spam mailings containing infected attachments. Once downloaded, these attachments infect the victim computer, introducing a virus infection. (Jiang, et al, 2009) This is a fast and easy way to spread the infection due to the large nature of spam campaigns which reach thousands of computers daily. (Achan, Xie, Yu, Panigrahy, Hulten, & Osipkov, 2008)

Lastly presented by Jiang, et al, (2009) is the automatic scan, exploit, and compromise approach. This is more like a brute force approach for spreading the infection, as it requires scanning IP addresses and ports across the internet looking for vulnerabilities to exploit to deliver the code. (Jiang, et al, 2009)

What Viruses Seek to Accomplish

Jiang, Li, and Zou (2009) discuss several attack mechanisms in their presentation of data. The first is compromising new hosts. This is carried out through various propagation mechanisms such as social engineering, spam e-mail containing malicious code, and the infection mechanisms discussed earlier. (Jiang, et al, 2009) The authors first discuss Directed Denial of Service attacks, which they state that mechanisms to carry out these attacks are common among viruses designed to create botnets, and are used to disrupt service at a site or to send thousands of legitimate requests to the site. Elliot (2000) also discusses these types of attacks in his article, noting how hard infected computers are to stop, as it is easy for attackers to take control of thousands of computers to institute the attack.

Spam attacks are the next in the list presented by Jiang, et al (2009). Spam bots often contain SMTP abilities which allow them to spoof e-mail addresses and send spam e-mail messages. (Jiang, et al, 2009) The authors state that most of today’s spam e-mail is sent by networks of computers infected with a botnet virus. This conclusion is supported by the experiments carried out by Achan, et al, (2008) in their look at spamming botnets. This research identified 7,721 spam campaigns, 580,466 spam messages, and 5,916 Autonomous Systems in what, in the grand scheme, was a relatively small portion of the attacks carried out on a daily basis.

The last two sets of attacks mentioned by Jiang, et al, (2009) are aimed at stealing information. The first of these is the Phishing attack. The authors note that by turning victims into web or DNS servers, they can be used to get sensitive information from others on the web. (Jiang, et al, 2009) On the other hand, Sensitive Data Stealing attacks are aimed at stealing information from the local victim machine. (Jiang, et al, 2009) Jiang, et al, state that this is done through several methods, including file uploading, key-logging, and screen capture software.

Guinier (1991) also provides a table (Table 1) which describes the presence of components of viruses (split up into Guinier's subcategories described previously) under the criteria of illicit action (Act), threshold mechanism (Thr), transfer mechanism (Tra), auto-replication process (Aut) and permanence (Per). Other attack mechanisms are discussed on a case by case basis in the next section.

Classification of the illicit objects

	Act	Thr	Tra	Aut	Per
Virus	Y	?	?	Y	Y
Worm	Y	?	Y	Y	N
Logical Bomb	Y	?	N	N	Y
Trojan Horse	Y	N	N	N	Y

Table 1
(Taken from Daniel Guinier's *Prophylaxis for "virus" propagation…* p.2, full citation in References)

Famous Viruses of the Past

In early 1989, many people had never heard of a computer virus. This all changed when the “Cornell virus” swept through the nation, bringing computer systems nationwide to a halt and prompting discussions about security policy, user rights and responsibilities. (Rotenberg, 1990)

Compared to the viruses of today, the earliest viruses were simplistic in nature. Instead of containing multiple attack mechanisms as discussed above, viruses were mainly created with one specific purpose (often prank like in nature,) instead of serving as an avenue for multiple attack types. The CHRISTMAs EXEC, for example, displayed a Christmas greeting to the victim upon being opened, and then sent itself to all of the user’s recent network contacts. (Kurzban, 1989) On the other hand, logic bombs such as Jerusalem and Michelangelo were programmed to destroy system data, the former deleting executables on the infected machine every Friday the 13th, and the latter overwriting hard disks on its namesake’s birthday. (Greiner, 2006)

However, it didn’t take long for things to progress from pranks to extensively harmful. The aforementioned Cornell virus, more commonly known as the Morris Worm, was released in 1988 when Cornell student Robert Morris misjudged the effects of a program designed to assess how big the internet was; a mistake that resulted in the first recorded denial of service attack. (Greiner, 2006)

Fast forward to the mid 1990s and we begin to see more innovation in virus techniques. The concept virus first exploited the macro language used by Microsoft Word to deliver payloads of malicious code, an idea later used by the Melissa virus. (Greiner, 2006) However, as Greiner presents in her article, this was not what made Melissa famous; instead, it was Melissa's position as one of the first viruses to use a combination of techniques to spread and attack victims.

Garber (1999) discusses Melissa's effects in depth in his article. The author states that Melissa not only infected the Normal.dot template (ensuring that future documents on the system would also be infected with the virus,) it would also send a message with an infected file to the first 50 contacts in the recipient's Outlook address book. The virus also contained a prank to insert a Simpsons quote in an open document when the minutes after the hour matched the date, as well as editing or disabling prompts and security settings regarding macros.

Greiner (2006) notes that the ILoveYou virus of 2000 was particularly noteworthy because of the social engineering aspect of the virus. The malware took advantage of default windows settings which hide the extensions for known file types. Therefore, when unsuspecting victims received a file named LOVE-LETTER-FOR-YOU.txt.vbs, they only saw the .txt extension and, wrongly, assumed it was a text file. Due to the fact that the virus sent itself to contacts in the recipient's e-mail address book, the victim usually received the infected file from someone they knew. This combination of known senders and trust for text files made for a very effective virus, and the author notes that many variants of the virus were quickly developed.

Viruses have continued to mutate and transform, and are only further exemplified in the case of the Conficker virus. This virus, despite an unprecedented global attempt at containing it, has eluded captors and has consistently been one step ahead of every concentrated effort. (Bowden, 2010) Infecting 6 million to 7 million computers, and having never been used to its full potential (Bowden, 2010), Conficker serves as a constant reminder that the war against viruses is being lost. It is safe to say that it is time for a new approach.

Literature Review

In order to attempt to understand several approaches to fighting cybercrime, three articles will be reviewed. The first presents a perspective of the attempt to apply traditional crime theory to cybercrime. The second is an argument against the application of the same crime theory on logical and fundamental principles. The third article looks at current approaches to combating cybercrime and suggests innovative new approaches to the fight against cybercrime.

Applying the Routine Activities Theory

Bossler and Holt (2009) undertake research in the application of routine activities theory (RAT) on cybercrime. The authors state that most research up to this point has focused on anti-virus and detection measures, and that in order for these methods to work properly, users must use them properly. Therefore, the two suggest that more research is needed into human behavior in the role of virus spreading and suggest that this can be done with RAT which has been successfully used to assess burglary. RAT states that direct-contact predatory victimization occurs when a criminal happens upon a victim who is without an appropriate level of guardianship. (Bossler & Holt, 2009)

In the next portion of the research, Bossler and Holt (2009) examine each component of the theory as applied to burglary and assess how the core concepts could be applied to cybercrime. First the researchers provide an overview of RAT. This includes an introduction to the aspects of the theory that revolve around the victim’s routine, different types of guardianship, and suitable targets. The authors state that research has suggested that an individual’s specific activities (for example, your daily work routine) are more inclined to cause burglary than the amount of time they spend doing those activities. Bossler and Holt also state that there are varying levels of guardianship including physical guardianship (locking your doors and setting an alarm), social guardianship (selecting your friends wisely and not making a habit of being around deviants), and personal guardianship (such as not informing people you will be out of town or your security key codes.) Lastly, the authors address suitable targets, which in burglary is someone who has expensive possessions and/or is monetarily wealthy.

At the beginning of their research, Bossler and Holt (2009) theorize that the above may be applied directly to cybercrime. Their thoughts are that someone's specific activities online (visited websites, illicit activities, etc.) will also be more important than the time they spend online in determining if they will become victims of cybercrime. The authors also theorize that physical guardianship (through things such as anti-virus), social guardianship (not being associated with those who are deviant in their behaviors online), and personal guardianship (such as updating products frequently and using private passwords that are complex) will also have a positive impact against infection. Lastly, the authors state that in the world of computer crime, everyone is a suitable target, as viruses infect victim computers indiscriminately and while they may be designed to impact one individual more than another, the impact is felt by all who are infected.

The research presented within this study provided some intriguing results. Bossler and Holt (2009) surveyed students on a college campus and studied 570 infections. The survey asked students about their online activities, how often they had spent doing them, how often they had been infected with a computer virus, and about any deviant behavior that they or their friends took part in. What the authors found correlated to some of their hypotheses, but not to others. To begin, Bossler and Holt (2009) found that physical and personal guardianship as well as routine activities did little to increase the rate of infection. However, the authors did find that some deviant behaviors (pirating media, hacking, and unauthorized network access) and absence of social guardianship (by hanging out with people who also participated in deviant behaviors) did correlate to an increase in infection. Some deviant behaviors (pirating software and pornography viewing) did not follow this trend, though in the case of pornography, associating with those who viewed it did put the respondent at a higher risk of malware infection. (Bossler & Holt, 2009) Lastly, the authors uncovered interesting demographic information which suggested that those who were employed also faced a higher risk of infection than those who weren't, and that being female increased the rate of infection among those surveyed as well.

Bossler and Holt (2009) use this data to suggest that there needs to be a multi-faceted approach to dealing with malware infections, and that both technological approaches and increases in behavioral awareness will be needed. The authors suggest that first, there should be a greater emphasis put on the connection between computer deviance and malware infection. This implies that effective campaigns directed at reducing piracy should focus on the impact on those doing the downloading (such as the risk the computer will be infected) rather than the impact on the music artist, as the impact on the artist is typically viewed to be small while the act of piracy has no negative impact on the end user. (Bossler & Holt, 2009) Lastly, the authors state that policy among service providers should focus on banning those who use the network for nefarious purposes (such as pirating) from having network access, as the research suggests a correlation between this behavior and increased malware infection.

An Argument Against RAT

There is a counter argument to the application of RAT to cybercrime as offered by Yar (2005). While the author admits that there are portions of RAT that appear applicable to cybercrime, the theory as a whole does not stand up in application. To prove this point, Yar begins by introducing the same theory presented above, but making special note of the spatial and temporal relationships that are required for the theory to hold water. That is, that the theory depends on the victim being in close proximity to the offender and that the victim must have a routine that produces a rhythm to which the criminal's actions sync, allowing the commission of a crime. (Yar, 2005) Further, the author illustrates through examination of various definitions of cyber crime, the singularity of cybercrime in that it can simultaneously affect thousands of users in an instant and that victims are always within immediate reach of the perpetrator. This leads Yar to surmise that the criminal behavior surrounding cybercrime is new and differs from that of traditional, established crimes.

Yar (2005) also examines at length the spatiality and temporality of cyberspace. The author notes that despite the presence of chatrooms, classrooms, and cafés, the geography of the internet is largely self imposed by the users in an attempt to relate what is boundless to the specific boundaries of our non-virtual world. This, Yar says, makes RAT a shaky theory, as it relies heavily on convergence in special relations and involves theory of distances and proximity, whereas the internet is without space and users are always within immediate reach. The author does concede, however, that the internet does include some notions of space: socio-economic factors separate users based upon connection availability; websites are created and/or viewed in physical space and therefore hold some amount of real world geography; while someone's internet presence may exist, it can often be difficult to locate. Yar states that while this slight bit of geography does exist, it can change within an instant through something as simple as a link being added to a page. It is this constantly changing topology that leads the author to say that applying RAT to cybercrime is difficult at best, as one of the foundations of the theory is based on spatiality of the world, victim, and perpetrator.

In the case of temporality, Yar (2005) finds similar fault with a second core tenant of RAT. The author notes that in cyberspace, there is no temporal routine; that internet users are connected to the internet at various times throughout the day for work, school, or leisure. The temporal routine theory is what leaves the victim or his or her property vulnerable with no one around to guard over it. (Yar, 2005) However, as Yar notes, there is a constant presence on the internet as people around the world connect, and therefore, the criminal is never left *totally alone* to carry out a crime.

Yar (2005) also evaluates targets as they are evaluated under RAT, on the basis of Value, Inertia, Visibility, and Accessibility. On the front of value, the author notes that value is largely in the eye of the beholder; an item acquired through illicit means may have social or economic value, but it is entirely what the criminal sees himself doing with it that makes it more or less valuable than anything else. In this way, Yar notes that the values of items on the internet are no different than the values of items in the physical world; the true value of data obtained through cybercrime will lie in what the perpetrator intends to do with it. However, this is the most closely related of the four variables in the author’s examinations.

When it comes to inertia, Yar states that in the physical world the size of an object or the size of a person makes them more or less likely to be stolen or attacked due to the dangers of the perpetrator being caught or injured. In the case of cybercrime, however, the only factors to inertia are connectivity speed and the size of a download, which given a good internet connection are easily mitigated. (Yar, 2005) In the case of visibility, the author notes, people or personal property items that are highly visible are more likely to be the target of crime. Yet, Yar states that on the internet (a public establishment,) people are equally visible, and that this visibility is present on a global level that isn't seen in traditional crime.

In the case of accessibility, the traditional RAT theory relates accessibility in terms of things such as a means of egress for the criminal. (Yar, 2005) However, due to the previously discussed spatiality issues, the author notes that all users are all equally accessible. Further, Yar states it is easy for a criminal to escape simply by disconnecting and going off the grid, or by using anti-traceback tools. The author does note that in terms of physical accessibility (locks or physical preventative measures in traditional crime) there is an equivalent in passwords and firewalls, though these can be circumvented as easily as they are in the physical world.

Lastly, on the topic of capable guardians, Yar (2005) finds that the concept is able to be applied to cyberspace. The author notes that social guardians are present through IT administrators and security organizations, as well as the general public. Yar also writes that the anti-virus and firewall programs tend to act as physical guardians do in RAT as applied to traditional crime.

The differences described above all lead Yar (2005) to conclude that while the conceptual work of RAT (victim, perpetrator, and guardians) may only contain differences of a smaller amount that require adjusting, the fundamental differences of temporality and spatiality are insurmountable. These differences, the author states, are enough that it is possible to conclude that cybercrime is not in fact "'old wine in new bottles' [but] 'old wine in *no* bottles' or, alternatively, 'old wine' in bottles of varying and fluid shape." (Yar, 2005, p. 424)

The Problems of International Cooperation

Lewis (2004) takes a different approach to examining the conundrum of cybercrime and how to fight it. The author begins his research by stating that all attempts at combating cybercrime that rely on international cooperation are doomed to fail. Therefore, within this work, Lewis states that he will examine the risks of computer crime and legal frameworks that fall short of being effectual deterrents to cybercrime.

The body of the research begins by noting that identity theft is on the rise, with 27.3 million Americans being victims to this crime in the 5 years before the writing. (Lewis, 2004, p. 1354) These statistics, Lewis states, are indicative of a greater rise in computer crime that is a global phenomenon. The threat posed, the author says, is one that not only affects individuals in their everyday life, but the security of the nations in which they live.

Lewis (2004) next introduces three attempts at international cooperation on the cybercrime front. The first of these is the G8 Ten-Point Plan. This plan, as the author describes, was developed by 8 major industrialized nations and was aimed at creating a greater law enforcement presence within those countries while also lending assistance to other, less developed, countries. The plan also calls for the nations to make cybercrimes illegal and to promote the investigation of these crimes within their borders. (Lewis, 2004) The next of these attempts is that of the Council of Europe Convention on Cybercrime. This convention encourages participating members to adopt legislation against cybercrime and attempts to foster international cooperation. (Lewis, 2004) One way which Lewis states the latter is accomplished is by requiring participating members in the convention to make cybercrimes offenses for which a perpetrator can be extradited from their borders. The third and final attempt presented by the author is the American Bar Association's Guide to Combating Cybercrime. This guide calls for uniformity in cybercrime laws among all nations and an increase in training law enforcement officials and cooperation in the investigation of cybercrimes on the international front. (Lewis, 2004)

The research also covers three distinct problems with attempts, such as those above, at fostering international cooperation in battling cybercrime. (Lewis, 2004) First, Lewis establishes that there is a lack of incentive for countries to participate. There are two distinct reasons that the author notes may result in a country not wanting to participate in such attempts. The first of these reasons is that a country may not have a large number of computer users, and thereby, the issue of cybercrime is a moot point. (Lewis, 2004) Secondly, Lewis states, the country may see it as beneficial to provide a safehaven for cybercriminals, whether it be due to bribes from criminals, the money they may receive from larger countries to fight the problem, or a sympathetic attitude toward terrorist activities.

Lewis (2004) also discusses the problems surrounding the effectiveness of such attempts. The author notes that global legislation cannot act as fast as the technology, and would thereby be reactionary and late. Further, Lewis notes, even when there are laws in place, it is difficult to harmonize the laws due to the fact that there are varying degrees of morality and legality throughout the world; what one country sees as a crime, another may not. Lastly, the author notes that cybercrime is borderless, while border disputes over extradition are common, and there is no governing body to require a country to participate in the agreement should they choose not to.

The last problem Lewis (2004) presents in relation to the globalization of cybercrime fighting is the opposition faced by the populace of countries. Within the United States, for example, the author notes that there is a growing opposition by the American Civil Liberties Union to the idea of government presence in the virtual lives of the populace. This is not limited to the United States, either, as similar opposition is also noted in Singapore. (Lewis, 2004)

Lewis (2004) thereby examines a few types of legal framework that could offer a solution to the problem. The first of these is the End-User Victim framework, in which the author proposes that it could be made such that investigation of cybercrimes was prioritized based upon what measures the end-user victim had taken to protect themselves. Therefore, if a user had taken no precautions, they would be shoved to the bottom of the pile behind those who had attempted to protect themselves through use of antivirus, firewalls, etc. (Lewis, 2004) The problem with this, Lewis notes, is that the cost of determining attempts made by end users would be extensive, and that some users may attempt to skate by on the security of the network as brought about by the good practice of other users on the network. This would leave a weak link that could potentially leave the entire network vulnerable due to one user's inaction. (Lewis, 2004) Therefore, the author suggests next an attempt at a Manufacturer and Software Maker framework. This framework, he notes, would provide regulations based upon flaws introduced by those who produce computer components and software, and hold them liable for defects and security holes that arose from their products. However, this may actually work as a disincentive to manufacturers who would be at an increased cost and less likely to try innovative approaches. (Lewis, 2004) This leads Lewis (2004) to another approach, focusing on a Would-Be Perpetrator and Cohort framework. Under this framework, there would be incentives (monetary or otherwise) for users to help in the capture of cybercriminals. (Lewis, 2004) The counterargument to this framework, presented by Lewis, is that it would cause criminals to be more secretive and thereby harder to catch in the long run than if such incentives were never offered.

The shortcomings of these three approaches lead Lewis (2004) to take a more in depth look at a framework based on internet service provider (ISP) incentives. The first of these is regulation requiring the best available technology to be present in the platforms of ISPs, giving the optimal protection to users. (Lewis, 2004) The problem with this, Lewis states, is that it is expensive, often monetarily wasteful, and further may push certain ISPs (such as academic institutions) out of their ability to offer internet service. This leads to the examination of a tort reliability regime, which the author notes would provide more flexibility for ISPs of varying sizes and inclinations, as well as discouraging improper protection by ISPs, encouraging better policies, and offering compensation to victims. However, the issue with this approach is that it puts the entire burden on the ISP and the criminal who causes the destruction shirks responsibility, while the ISP is left without a concrete framework to allow them to know exactly what they need to do in order to not be liable. (Lewis, 2004)

These failings cause Lewis (2004) to examine the problem from two more creative approaches. The first of these is by Hack-In Contests, which the author notes would encourage ISPs and manufacturers to hold contests where hackers are offered a prize for successfully hacking into their network, exposing security flaws before they are released to the public, and potentially extra incentives for suggesting ways to solve the issues raised. However, Lewis notes that this would require contracts in which the hackers were required to divulge all defects they found. Further, hackers may be disinclined to expose themselves to law enforcement officials and, similarly, corporations may be unwilling to work with those who generally seek to do them harm. (Lewis, 2004) Therefore, Lewis suggests a framework in which a Market Trading System, similar to that employed in emissions trading, be employed for fighting cybercrime. Under this framework, ISPs would be offered credits (based upon the size of the ISP and other factors) that would allow for a certain number of attacks or amount of damages caused within a timeframe. (Lewis, 2004) Should the company run out of credits, Lewis states, they would either have to purchase them from more secure ISPs, or they would face penalties and fines. This would allow for incorporation of all ISPs as well as punishing those who perform poorly while rewarding those who perform exceptionally. (Lewis, 2004) However, Lewis states that even this approach is flawed in that it still puts all responsibility for the crime on the shoulders of the ISP while the hacker escapes, and that reporting of attacks and damages would have to be mandatory by law for the framework to be effective – something that ISPs, manufacturers, and industry leaders are already wary of doing.

Lewis (2004) concludes that while none of the approaches are perfect, it is clear that a preventative framework is needed. The author states that even the best attempts at international cooperation are destined to fail at the onset; that it is only through a preventative framework that we can incorporate any or all of the above solutions in an attempt to prevent computer crime.

Discussion

From the overview of viruses given previously and the immediately preceding literature review, one thing is clear: there is no one *right solution.* The question often posed is 'How do we stop virus writers?' However, as the literature and statistics suggest, perhaps the better question is 'How do we mitigate the damage of viruses and eliminate the risk of contracting them in the first place?' While capturing those who perpetrate computer crime should never be a foregone conclusion, the attempt to steel ourselves against the effects of computer crime may be the best approach at the crossroads we have come to.

It is a certainty that the current approach to cybercrime is failing. As Lewis (2004) noted in his research, computer crime is on the rise, which is verified in the crimes recently reported to IC3 (2009). The problem of viruses is no exception to these shortcomings, which are exemplified in comparison of the number of viruses released into the internet against the number of convictions of virus writers. In the history of the internet, an estimated 63,000 viruses have caused approximately $65 billion worth of damages. (Techrepublic, 2003) Despite these staggering numbers, very few virus writers have been captured and convicted (Gordon, 2000), and in those instances where they have, the penalties imposed upon the perpetrators have been small compared to the amount of damage caused by their code. (Techrepublic, 2003)

There are some important points to be taken from the research above. The first of these is that computer crime, though at first glance similar to that of traditional crime, is a crime that we must approach in new and innovative ways. While we may be able to find some instances in which our crime theories fit, for the most part, they will fail to fully explain the root cause and effect of cybercrime. This is proven both empirically by Bossler and Holt (2009) and logically in the work of Yar (2005.) In the case of the former, it is clear that while some criteria of RAT met the surveyed sample of students, there were certain aspects (in terms of physical and personal guardianship together with routine activities) that did not fit the mold of the theory. Similarly, the latter study clearly shows a disconnect between the founding principles of RAT and what we can observe in an online environment.

Further still, it is clear from both the reviewed literature and the technical overview presented previously that viruses are indiscriminate in who they affect. All users of the internet are just as likely as the next to be impacted by a virus. This means that we have little ability to successfully predict who a criminal may target as the targets may not have been intended in the first place. As shown by several of the viruses presented by Greiner (2006), often times a virus writer does not know who the virus will infect, simply that it may affect the first x number of contacts in a user's address book. Therefore, a virus placed on one website may affect one or a million users, any or all of which may be exploited by the virus writer when the infection takes hold.

These differences uncover a fundamental flaw in attempting to apply law that is based in a physical space to crimes that occur in an area unbounded by the normal rules of geography, law, moral standards, or criminal targeting. The internet is a frontier that cannot be governed in the same way that we govern the physical plane. Therefore, it becomes increasingly obvious that in order to fight a fundamentally new crime, we must take a fundamentally new approach.

As a whole, we have been trying since the advent of the virus to fight the problem in a reactionary method. As Lewis (2004) suggests, a preventative measure seems to be the next logical approach. While Lewis finds fault (to some extent) with each of the methods he presents, there are some ways in which the ideals may be combined in order to form a good preventative framework. For example, if a framework of a Market Trading System were to be established, it could be combined with incentives for catching criminals, such as what is seen in the Would-Be Perpetrator and Cohort framework. In this sense, instead of rewarding the friends and companions of perpetrators who helped to capture criminals, the organizations, manufacturers, or ISPs involved in the capture of the criminals could be given credits towards their share of the market trading platform. These incentives combined with an increase in the prosecution rates and penalties for those convicted of cybercrime could help to deter criminals from turning to cybercrime in the first place. In this way, not only would we be rewarding or punishing ISPs based upon their performance, the onus of responsibility would be equally shared among ISPs who provide the service and the criminals who commit the crime. This could be even further combined with a variation on Lewis' (2004) End-User Victim framework by giving courts the freedom to determine the amount *civilly* that any ISP or cybercriminal can be held responsible for their actions based upon the extent that the end-user attempted to protect themselves from the attack. This as well gives the incentive for end-users to protect themselves without requiring extra time and expenditure from a taxed law enforcement, as these types of investigations would normally be undertaken in discovery for a civil court case.

This is not to say that this approach is without flaw. This attempt at a framework does not address a global level of cooperation that would still be needed for prosecution of crimes, or the problem of developing country safehavens. However, it is important for us to understand that as Lewis (2004) states in his work - continued focus in this area is destined to fail. The system above would be able to be adapted to countries across the globe based upon their own definitions of morality and criminality, and could be adopted in much the same way that the emissions system has been adopted by several countries around the globe. (Europa, 2010; Lewis, 2004) Such measures would be the start of a true global effort to combat cybercrime and bring virus writers to justice.

Summary and Conclusions

Viruses have become an expansive and growing problem for the internet and its users from the earliest days of the internet until now. Viruses have grown and mutated from simple pranks to incredibly destructive forces. The attempts to fight this computer epidemic have largely, up to this point, been reactionary and founded on principles of globalization that fail to stand the test of action. These seemingly failed attempts have yet to result in an end to the problem of computer viruses. As such, scholars have begun to question whether or not cybercrime is a traditional or new crime.

Studies presented in this work make it clear that the problem of cybercrime is something that is entirely new in the way it presents itself, due in large part to the structure and presence of *cyberspace.* As such, traditional crime theories fail to give us a clear explanation or plan of action to fight cybercrime and virus writers.

This suggests that in order to be effective our focus needs to shift from traditional crime and traditional reactionary measures to a more preventative approach. This approach, which may involve a combination of factors, incentives, and punishments to criminals, vendors, and consumers alike, may be the key to slowing the growth of computer crime. While there may never be a full solution to viruses or other forms of cybercrime, a preventative measure may at least be a way to mitigate the losses that are incurred when a cybercriminal attacks.

References

Achan, K., Xie, Y., Yu, F., Panigrahy, R., Hulten, G., & Osipkov, I. (2008). Spamming botnets: signatures and characteristics. *ACM SIGCOM Computer Communication Review , 38* (4), 171-182.

Ashmanov, I., & Kasperskaya, N. (1999). The virus encyclopedia: reaching a new level of information comfort. (H. Vin, Ed.) *IEEE Multimedia , 6* (3), 81-84.

Bossler, A., & Holt, T. (2009). On-line activities, guardianship, and malware infection: an examination of routine activities theory. *International Journal of Cyber Ciminology , 3* (1), 400-420.

Bowden, M. (2010, June). *The enemy within*. Retrieved July 20, 2010, from The Atlantic: http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/

Cheng, H., & Ma, L. (2009). White collar crime and the criminal justice system: government response to bank fraud and corruption in china. *Journal of Financial Crime , 16* (2), 166-179.

Cradduck, L., & Mccullagh, A. (2007). Identifying the identity thief: is it time for a (smart) australia card? *International Journal of Law and Information Technology , 16* (2), 125-158.

Elliot, J. (2000, March/April). Distributed denial of service attacks and the zombie ant effect. *IT Pro* , 55-56.

Europa. (2010, March 22). *Environment - climate change - emission trading system*. Retrieved July 20, 2010, from Europa Environment: http://ec.europa.eu/environment/climat/emission/index_en.htm

Garber, L. (1999). Melissa virus creates a new type of threat. *Computer , 32* (6), 16-19.

Gordon, S. (2000). *Virus writers: the end of innocence?* Retrieved July 31, 2010, from CiteSeerX: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.61.2835

Greiner, L. (2006). The new face of malware. *netWorker , 10* (4), 11-13.

Guinier, D. (1991). Prophylaxis for "virus" propagation and general computer security policy. *ACM SIGSAC Review , 9* (3), 1-10.

Higgins, G., Wilson, A., & Fell, B. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture , 12* (3), 166-184.

IC3. (2010). *2009 internet crime report.* Washington D.C.: National White Collar Crime Center.

Jiang, W., Li, C., & Zou, X. (2009). Botnet: survey and case study. *2009 Fourth International Conference on Innovative Computing, Information and Control* , 1184-1187.

Kurzban, S. A. (1989). Defending against viruses and worms. *ACM SIGUCCS Newsletter , 19* (3), 11-23.

Levy, E. (2003). The making of a spam army. *IEEE Security & Privacy , 1* (4), 58-59.

Lewis, B. (2004). Prevention of computer crime amidst international anarchy. *The American Criminal Law Review , 41* (3), 1353-1372.

Li, P., Wang, Z., & Tan, X. (2007, December). Characteristic analysis of virus spreading in ad hoc networks. *Computational Intelligence and Security Workshops, 2007.* , 538-541.

Mavrommatis, P., Provos, N., Rajab, M. A., & Monrose, F. (2008). All your iframes point to us. *17th USENIX Security Symposium* , 1-22.

Microsoft. (2006, October 23). *What is a computer virus?* Retrieved July 20, 2010, from Microsoft.com: http://www.microsoft.com/nz/protect/computer/basics/virus.mspx

Rotenberg, M. (1990). Prepared testimony and statement for the record on computer virus legislation. *ACM SIGCAS Computers and Society , 20* (1), 12-25.

Simmons, B. (1999). From the president: melissa's message. *Communications of the ACM , 42* (6), 25-26.

SpyChecker. (2009). *What is spyware and adware?* Retrieved July 20, 2010, from SpyChecker.com: http://www.spychecker.com/spyware.html

Techrepublic. (2003, September 25). *Who writes viruses?* Retrieved July 31, 2010, from ZDNet UK: http://www.zdnet.co.uk/news/security-management/2003/09/25/who-writes-viruses-39116671/

Yar, M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology , 2* (4), 207-427.

Zhang, X., Saha, D., & Chen, H.-H. (2006). Analysis of virus and anti-virus spreading dynamics. *Global Telecommunications Conference, 2005. , 3*, 5.