Jordan Wright IE 5320 R10177180

A Systems Analysis of the Cybercrime Industry

November 26, 2013

Table of Contents

Abstract

In recent years, the underground economy surrounding the cybercrime industry has undergone a structural and systematic shift into a mechanized organismic system. This system allows for fraudsters specialized in a particular role to contribute to the flow of goods sold. This specialization has resulted in the separation of the manufacture and monetization of compromised hosts and personally identifiable information (PII). By utilizing the techniques and method provided by general systems theory, interactions that occur within the system can be understood, future changes in the system can be predicted, and weaknesses in the systems structure can be enumerated. Specifically, through causal loop analysis, it can be determined that the supply chain model in use by fraudsters suffers from the Tragedy of Commons (TOC) archetype, which can be exploited to weaken the system, as well as suggest that existing estimates of the system's profitability may be exaggerated. Additionally, due to the structure of how goods are sold between producers and consumers in the industry, isomorphisms can be discovered between cybercrime and traditional "lemon markets". By understanding these isomorphisms, researchers and law enforcement can introduce actors into the system which can change the system in order to hinder the system behavior and efficiency, potentially reducing further cyber fraud.

1. Introduction

It is estimated that more than 2.7 billion individuals utilize and store information about themselves on the Internet on a regular basis[i]. The use of Internet services such as social media, e-commerce, and online banking requires users to submit sensitive personally identifiable information (PII) about themselves to be stored by the service provider. In addition to this, corporations are increasingly outsourcing the storage of valuable intellectual property (IP)[ii]. The centralized storing of PII and IP by third party providers has created an opportunity for hackers, identity thieves, and fraudsters to commit identity theft on victims or theft of valuable corporation assets.

The opportunity to commit cybercrime, combined with the development of sophisticated tools and techniques, has driven fraudsters to create a distributed, organized, and highly anonymous international system with each individual providing a unique service to facilitate fraud. This system has since evolved into an illicit underground industry estimated in 2013 to be "measured in the hundreds of billions of dollars"[iii] (McAfee, 2013). With many actors and components interacting within the supply chain process, it is overwhelming to study the industry using traditional methods. However, using systems analysis techniques, isomorphisms between current cybercrime organizations and "lemon markets" can be discovered. In addition to this, by studying the supply chain management in use by the industry using causal loop diagrams, one can discover the existence of system archetypes which may assist in understanding the behavior and future profitability of the system. Both the causal loop diagrams as well as the isomorphisms to lemon markets can be used by researchers and law enforcement in an attempt to discover weaknesses within the system which could be used to hinder or disrupt the system's functionality, preventing further fraudulent activities.

2. Summary of Project Situation

2.1 History of Cybercrime

It is beneficial to begin analysis of this industry by briefly examining the evolution of cybercrime into the current "Exploit as a Service" (EaaS) model that exists today. The first computer virus, called *Creeper*, was released as an experiment in "self-replicating… software" in 1971[iv] (Totty, 2011). Until the end of the 20th century, most subsequent viruses or cyber-attacks were written or performed as "attempt[s] at gaining bragging rights and notoriety"[v] (McAfee, 2011). However, as Internet services became more widespread and sophisticated, criminals "who used to seek exploits for recreation or reputation have given way to those who are in it for the money."[vi] (Herley, Florencio, 2009).

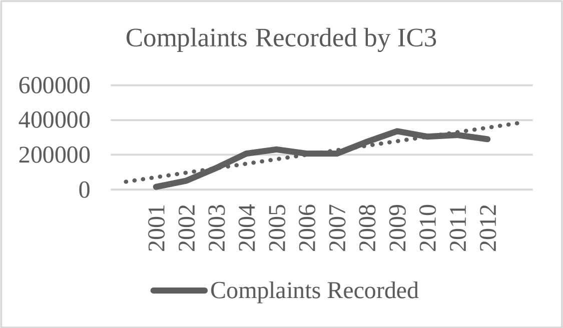

Figure 2 (Data Source: IC3 Annual Reports)

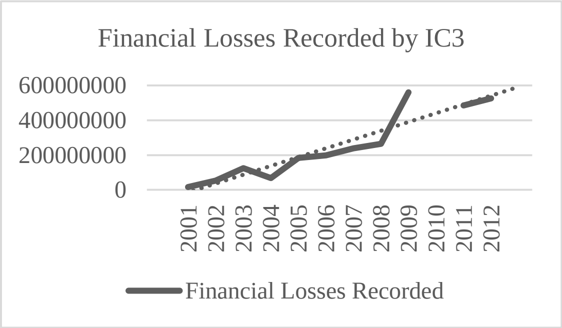

Figure 1 (Data Source: IC3 Annual Reports)

This industry proved to be profitable to fraudsters. In an attempt to combat the rapidly expanding practice of cyber fraud, the US government established the IC3 and US-CERT organizations in 2000 and 2002, respectively[vii][viii]. In its 2001 Annual Report, the IFCC – since renamed to the IC3 – recorded nearly 17,000 complaints of cyber fraud, resulting in $17.8 million in losses[ix] (IC3, 2001). The large majority of complaints recorded by the IFCC were due to auction fraud, in which attackers post assets for sale on popular online auction sites such as eBay[x] and, when the item is bought by a customer, fail to send the item to the buyer and refuse to issue a refund. Since the initial report published in 2000, nearly each subsequent annual report published has seen an increase in both the number of complaints recorded, as well as the recorded losses to individuals and businesses as a result of the complaints.[xi] The results from these reports can be seen in Figure 1 and Figure 2. This increase in the number of online criminal activities is comparable to those of traditional fraud. Namely, we can see that fraud activity occurs "where the money is"[xii], and cyber fraud is no different.

2.2 Shift to Targeting Personally Identifiable Information (PII)

As more individuals started using increasingly sophisticated Internet services on a daily basis, more valuable information was beginning to be stored by both service providers as well as consumers directly. This information could range from simple usernames and passwords, to PII such as social security numbers (SSNs), bank account information, or credit card numbers (CCNs). Attackers quickly realized that by shifting tactics and focusing on obtaining this sensitive information from both the individuals themselves, as well as from the service providers, they could maximize their profits by selling the PII to identity thieves who will use the information to obtain unauthorized access to the monetary assets of each victim. Standard prices found for different types of PII can be found in Table 1. These prices depend on the amount of information provided, such as the PIN, SSN, etc.

Asset	**Price**	**Data Source**
American Credit Card Number	\$15 - \$200	McAfee® Labs, 2013[xiii]
European Credit Card Number	\$40 - \$250	McAfee® Labs, 2013
Canadian, Australian Credit Card Number	\$25 - \$200	McAfee® Labs, 2013
Asia Credit Card Number	\$50-\$190	McAfee® Labs, 2013
US bank account with full information	2% of balance	McAfee® Labs, 2013

European bank with full information	4-6% of balance	McAfee® Labs, 2013
PayPal	6 – 20% of balance	McAfee® Labs, 2013
Western Union Transfer	10% of amount	McAfee® Labs, 2013

Table 1 - Prices for stolen assets

Criminals began to employ numerous techniques in order to compromise the computers and networks both individuals and service providers. The most prolific technique used by attackers is "phishing", accounting for 51.2% of the attacks report by US-Cert in 2011.[xiv] To perform phishing attacks, fraudsters send an email to victims purporting to come from a trusted source. The email, when opened, will either use multiple techniques in an attempt to infect the victim's computer with special software designed to steal information called "malware", or attempt to social engineer the victim into divulging sensitive information to the attackers directly. Examples of the techniques used to install malware on victim hosts include requesting the victim to open a malicious attachment, or directing the victim to a malicious website controlled by the attacker which, when visited, exploits the user's browser to compromise the host. The rise in profitability and popularity of this industry among fraudsters drove the creation of increasingly sophisticated malware. Among these, one particular piece of malware called Zeus, allegedly discovered in 2007[xv] and subsequently resurfaced in 2009[xvi] under the pseudonym "ZBot", marked a change in the functionality of malware. This new family of malware, called "banking Trojans", were designed to not only give attackers persistent backdoor access to the compromised host, but also to automatically obtain and report sensitive such as online banking credentials to the attackers.[xvii] The introduction of banking Trojans gave fraudsters assets to be sold, which created a shift in the organizational structure and flow of goods in the cybercrime industry.

2.3 Development of Organizational Structure

As the process to commit cyber fraud became more widespread and sophisticated, "miscreants readily apprehend[ed] that tackling the entire value-chain from malware creation to monetization…pose[d] a daunting task requiring highly developed skills and resources"[xviii] (Caballero et. al., 2011). This facilitated one of the first major shifts into the organizational structure of the underground industry we observe today. Namely, this created specialized roles among fraudsters, in which there exists "buyers and sellers, intermediaries and even service industries”[xix] (Zeller Jr., 2005) working together to provide the flow of goods and services needed to commit fraud. This increase in specialization and interaction between parties evolved the existing individual-oriented structure into a more systematic and organismic structure, or “whole”. In fact, as it will later be shown in depth, the evolution of this distributed organization follows the same pattern of organismic organization originally proposed by Bertalanffy[xx]. It can be observed that to analyze such a system, we will indeed need to utilize the methods and techniques of general systems theory.

3. Analysis of Cybercrime Industry

3.1 The Cybercrime Industry as an Organismic System

To analyze the cybercrime industry using general systems theory techniques, we will first observe the evolution of the organismic organizational structure that exists today. Bertalanffy originally posits that, for organismic systems, “progress is possible only by subdivision of an initially unitary action into actions of specialized parts.” (Bertalanffy, 1968). We can observe this phenomenon holds true in the cybercrime industry as actors were progressively “segregated” into specialized roles. Actors within these specialized roles were then subsequently “mechanized” to create microsystems within the roles. For example, malware authors would commonly discuss new tools and techniques to create increasingly sophisticated and effective malware for their customers. However, we can also observe that the flow of goods between each mechanized subsystem creates interactions which work together towards the entire centralized and individualized industry.

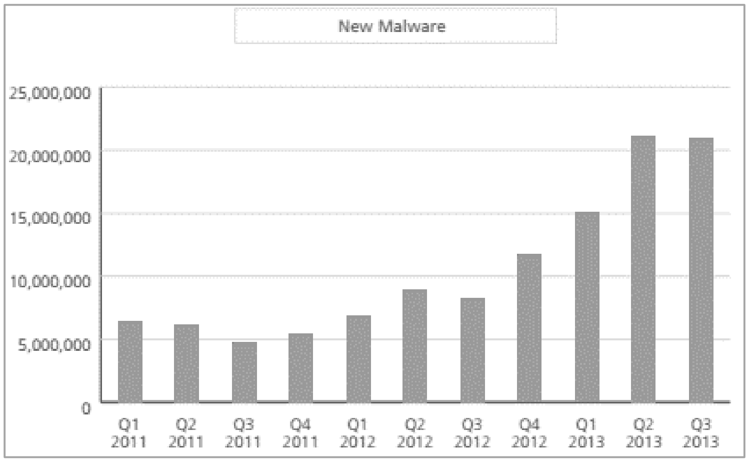

Figure 3 - New Malware (source: McAfee® Labs Threats Report: 2013 Q3)

As Bertalanffy originally predicted, this mechanization provided progress to the already advancing industry. The progress resulting from this change in organizational structure can be seen in Figure 3 (McAfee® Labs, 2013), which shows the results from the McAfee® Labs Threats Report for the third quarter of 2013[xxi]. It is observed that the malware industry is expanding at a rapid pace, with over 20 million samples discovered in Q3 2013. In addition to this, this evolution of the organizational structure facilitated the creation and adoption of new supply chain models for fraudsters to maximize the production and monetization of goods.

3.2 Analysis of the Flow and Monetization of Goods

3.2.1 Isomorphism to "X as a Service" Model

The increase in computing power coupled with the decrease in computing cost has given rise to "cloud computing". Summarized from the official NIST definition as "enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources"[xxii], cloud computing is an industry which allows businesses and consumers to outsource the often laborious process of creating and maintaining software, platforms, and infrastructure to service providers. These services are commonly referred to as "Software as a Service" (SaaS), "Platform as a Service" (PaaS), and "Infrastructure as a Service" (IaaS), respectively[xxiii]. Each of these service models are intended to abstract the implementation details away from customers in an attempt to separate the labor required to implement the solution from the value obtained by using the solution. As the cybercrime industry evolved into a specialized organismic system, fraudsters created models isomorphic to the existing cloud computing models to distribute and monetize their stolen or compromised assets. The model created and adopted in the cybercrime industry is known as the "Exploit as a Service" model.[xxiv] In this model, the "compromise" of victim computers and networks is strictly "decoupled from host monetization" (Grier et. al., 2013).

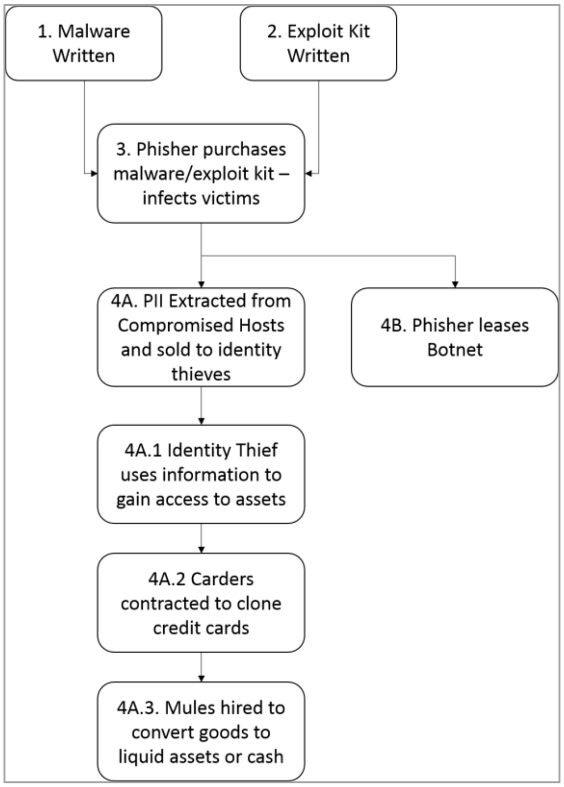
1. Malware Written
2. Exploit Kit Written
3. Phisher purchases malware/exploit kit – infects victims
4A. PII Extracted from Compromised Hosts and sold to identity thieves
4B. Phisher leases Botnet
4A.1 Identity Thief uses information to gain access to assets
4A.2 Carders contracted to clone credit cards
4A.3. Mules hired to convert goods to liquid assets or cash

Figure 4 - Flow of Goods and Services

The flow from the creation and manufacture to the monetization of goods is illustrated in Figure 4. This model represents the system in its current state, assuming a different actor for each specialized role. (1) The malware author creates malware (such as the Zeus crimeware toolkit[xxv]) designed to infect a host system and provide a backdoor for persistent access in the future. (2) A malware author creates an "exploit kit" (such as the well-known Blackhole exploit kit[xxvi]), which is code designed to be placed on a malicious website which, when visited by the victim, aims to exploit the victim's Internet browser using publicly known vulnerabilities. If the exploitation is successful, then the exploit kit downloads and installs the malware created in (1). It is important to observe that the author of the exploit kit could be a separate party than the author of the malware described in (1). This subsequently enforces the "progressive mechanization" principles introduced by Bertalanffy, in that subsystems can be further mechanized into even smaller subsystems in order to promote further progress. (Bertalanffy, 1968). (3) A phisher purchases a license for both the exploit kit and malware. Then, the phisher crafts a malicious webpage utilizing both of the assets purchased. The phisher then sends phishing emails to victims which, when opened, direct the user to the malicious webpage, and install the malware. Multiple compromised hosts are maintained and managed by the phisher in an organized structure called a "botnet". (4A) The botnet uses the installed malware to extract and harvest PII located on the compromised systems and sells them to identity thieves. (4A.1) The identity thief uses PII such as online banking credentials and credit card information to obtain unauthorized access to the victim's monetary assets. (4A.2) The identity thief contracts "carders" - fraudsters who specialize in the creation of cloned credit cards – to create clones of the victim's credit cards. (4A.3) The identity thief then hires "mules" to make withdrawals using these cloned assets to convert them to cash, which is then sent to the identity thief. (4B) The botnet master may also lease out control of some or all of the botnet to other botnet masters or spammers for a limited period of time.

A brief case study of this process can be found in the 2013 indictment of five fraudsters charged with gaining unauthorized access to multiple organizations including NASDAQ, Dow Jones, and 7-Eleven.[xxvii] After installing malware on the compromised systems, the fraudsters harvested over 160 million credit card records, which were subsequently sold to "cashers" (or carders) who "encoded each dump onto…a blank plastic card and cashed out the value of the dump by either withdrawing money from ATMs…or incurring charges and purchasing goods." (FBI, 2013). The fraudsters used the manufacture and flow of goods shown in Figure 4 to cause "in excess of $300 million by just three of the Corporate Victims, and immeasurable losses to the identity theft victims' (FBI, 2013).

3.2.1.1 Isomorphism to "SaaS" Model

The distribution of malware closely resembles the Software as a Service model. Authors of malware such as Zeus and the BlackHole exploit kit commonly use a "licensing model" to distribute copies of the malware. Consumers will purchase a license to use the software for a limited period of time measured in days, weeks, or even months. These licenses, depending on the malware and license period purchased, can cost consumers "in the order of several thousands of dollars" (ESET, 2013)[xxviii]. Within the licensing period, consumers will have access to updates and support from the providers. A diagram describing this process is shown in Figure 5. The isomorphism between this process and the SaaS model is clear in that the behavior is the same, which evokes similar change and evolution in the systems, such as the increase in software quality and sophistication.

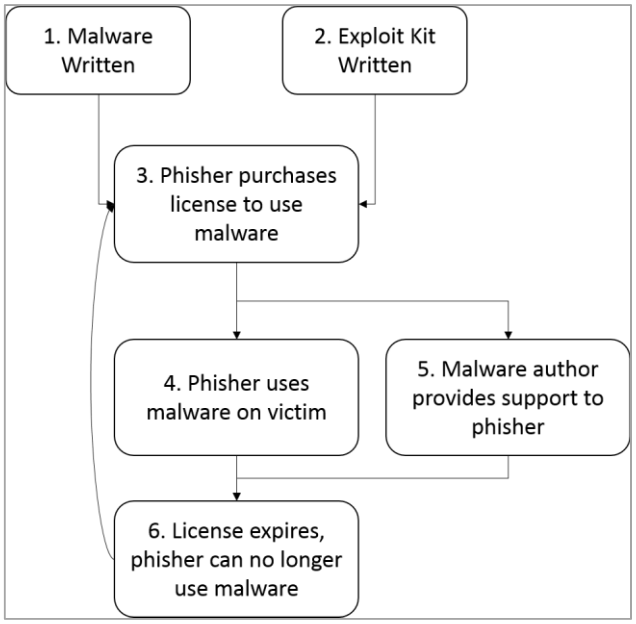
1. Malware Written
2. Exploit Kit Written
3. Phisher purchases license to use malware
4. Phisher uses malware on victim
5. Malware author provides support to phisher
6. License expires, phisher can no longer use malware

Figure 5 - SaaS Isomorphism

3.2.1.2 Isomorphism to "PaaS" Model

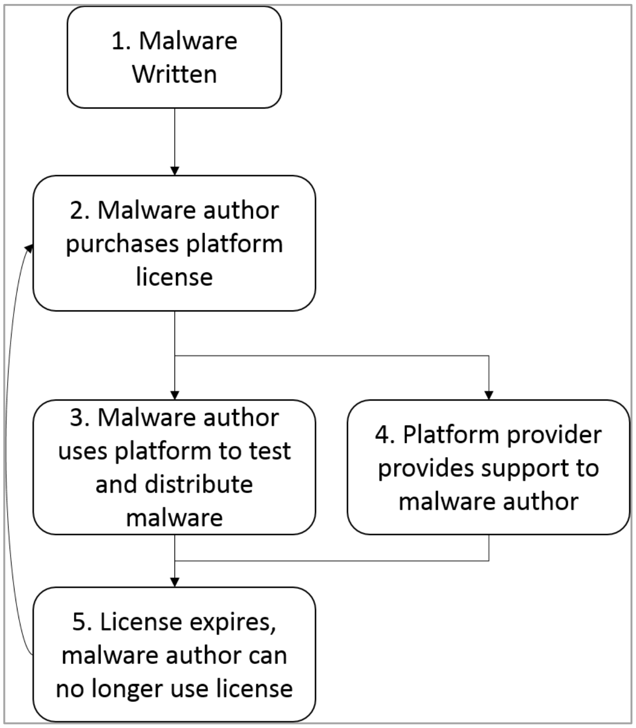
1. Malware Written
2. Malware author purchases platform license
3. Malware author uses platform to test and distribute malware
4. Platform provider provides support to malware author
5. License expires, malware author can no longer use license

Figure 6 - PaaS Isomorphism

Botnets can range substantially in size. Symantec recently released a report describing their efforts to dismantle the ZeroAccess botnet that had a "population upwards of 1.9 million computers"[xxix] (Symantec, 2013). With so many compromised hosts under their control, phishers can offer a platform to malware authors to purchase licenses to quickly distribute their malware to compromised hosts. These hosts can then be used by the malware author as a test-bed for their malware, or to further compromise additional hosts. The flow diagram describing this process in shown in Figure 6. This behavior is isomorphic to the existing PaaS model, in that the platform provided by botnet masters allows malware authors to test their malware in environments they don't need to setup. This isomorphism results in similar changes between the systems, as platforms can become more generic and sophisticated with their increased use.

3.2.1.3 Isomorphism to "IaaS" Model

In a similar way, botnet masters can also lease out or sell the botnet infrastructure directly. Consumers can then use this infrastructure to conduct their own phishing attacks, denial of service (DoS) attacks, or facilitate the spread of additional malware. This leasing of infrastructure is structurally similar to the IaaS model of cloud computing, and isomorphic changes can be seen in both. For example, as the scalability of service providers increases, a decrease in price can be observed. However, prices for compromised hosts are much lower than prices for legitimate cloud based hosting. In addition to this, while legitimate hosts are often leased "per instance", such as the case with Amazon EC2 cloud services[xxx], botnet infrastructure is often leased in groups of instances. At the time of this writing, the smallest available EC2 instance is priced at $.020/hour (Amazon, 2013). A report published by Trend Micro shows that hosts "consistently online 40% of the time"[xxxi] can be purchased for "$200 for 2,000 hosts" (Trend Micro, 2013). In this case, purchasers would be buying the compromised hosts, as opposed to leasing them. The flow of the goods presented in this model is shown in Figure 7.

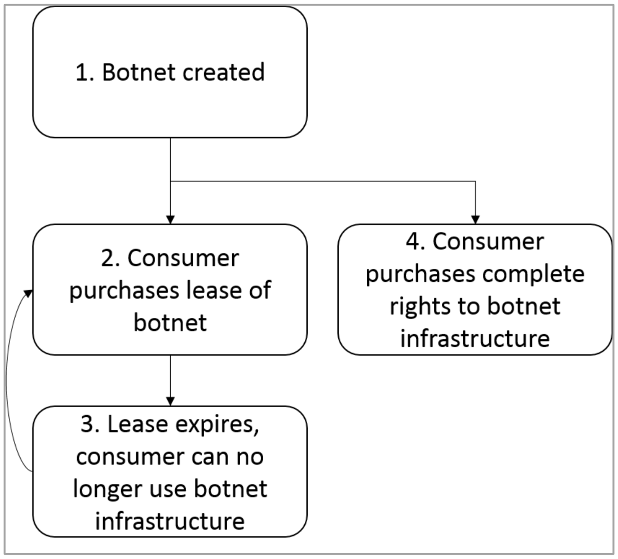
1. Botnet created
2. Consumer purchases lease of botnet
3. Lease expires, consumer can no longer use botnet infrastructure
4. Consumer purchases complete rights to botnet infrastructure

Figure 7 - IaaS Isomorphism

3.2.2 Anonymity Creates Lemon Markets

One of the primary traits of the cybercrime industry is that of anonymity. The anonymity provided by these markets is layered, in that all aspects of the transaction are performed as anonymously as possible. Producers and consumers often only know one another by a username or nickname. Communication largely takes place online in Internet Relay Chat (IRC) chat rooms, Internet forums and, if necessary, email. In addition to this, anonymity is largely stressed when it comes to the currency used to make transactions. Multiple currencies have historically been used to provide anonymity when making transactions. E-gold, WebMoney, Liberty Reserve, Perfect Money, and Western Union have all been used by fraudsters to both facilitate transactions as well as convert received assets to cash.[xxxii] Most recently, the use of cryptocurrency Bitcoin has been adopted by cybercriminals and other miscreants in underground economies (such as popular and recently taken down Silk Road underground market) due to its anonymity and easy conversion to cash and other liquid assets.

This anonymity, while desired among members performing illicit activity, also establishes a direct isomorphism to “lemon markets”. Originally introduced in a paper by George A. Akerlof[xxxiii], lemon markets refer to situations in which there exists asymmetrical information between buyer and seller with regards to the quality of assets for sale. Akerlof posits that the salesman of a used car knows more about that the quality of the car than the buyer, and can determine if the vehicle is of poor quality, or a “lemon”. Therefore, the salesman can exploit this knowledge through dishonesty about the car’s actual quality. A report published by Microsoft demonstrates that the underground economy satisfies the conditions to be considered a market for lemons due to the asymmetry of information between producers and consumers, lack of credible disclosure, rampant practice of fraud from sellers, and the lack of quality assurance or regulation.[xxxiv]

Indeed, it can be observed that the anonymity between sellers creates conditions ripe for a market for lemons. Sellers offering PII such as online banking credentials, credit card information, etc. have the ability to determine the actual value of these accounts before selling the assets to the consumers. The sellers can determine if the accounts associated with the PII are “lemons” or not before they advertise to sell them to buyers. In addition to this, the buyer usually will have no indication of whether or not the seller will follow through with the assets once the funds are received. There is also very little reason for sellers *not* to be dishonest. A causal loop diagram demonstrating this is illustrated

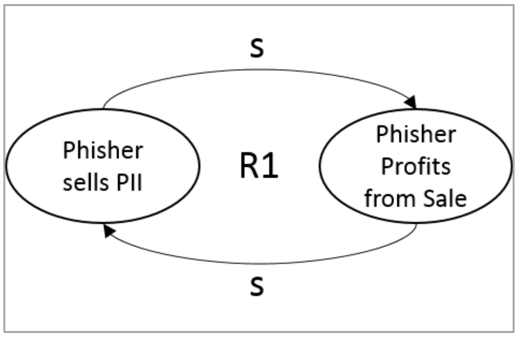

Figure 8 - Profit of Phishing Sales

in Figure 5. It can be observed that, by selling the same goods to multiple buyers, a reinforcing loop is created to give profit to the phisher, as there is no way for the buyer to be immediately aware that the goods are being subsequently sold elsewhere. This allows the phisher to obtain the same profit for each sale made.

It can be observed that the industry is isomorphic to lemon markets, in that similar change can be seen in both. Akerlof describes this change that occurs within lemon markets in that "the presence of people who wish to pawn bad wares as good wares tends to drive out the legitimate business" (Akerlof, 1970). This process of change also illustrates the open-systems principle introduced by Bertalanffy of equifinality, in which "the same final state may be reached from different initial conditions and in different ways." (Bertalanffy, 1969). We can see, if Akerlof's final model is correct, then the final state does not depend on the initial state. If enough dishonest actors are interacting within the system, legitimate business will be driven away.

This trait of the cybercrime industry could be exploited by researchers to potentially weaken the integrity of the market. By introducing intentionally dishonest actors into the system, it is possible to manipulate the state of the system such that the legitimate business is outmatched in scale. Since many of the currencies used by fraudsters intentionally allow the refusal of refunds, these actors could create dishonesty by providing fake goods and refusing to offer refunds to the upset customers. This would further substantiate the already existing mistrust between actors, removing legitimate business from the industry. This will result in financial losses amounting to both the losses "which the purchaser is cheated" as well as the "loss incurred from driving legitimate business out of existence" (Akerlof, 1970).

3.2.3 Enumerating System Weaknesses Using Causal Loop Analysis

Now that we have observed the general supply chain models in use by the cybercrime industry, we can use systems theory techniques in an attempt to find additional weaknesses in the system. A causal loop diagram representing the interactions that occur within the system is shown in Figure 6. (R1) Malware authors create malware (both exploit kits as well as the full payload), and sell it to phishers for a profit. The profit received from this malware provides the resources needed to create more sophisticated malware. (R2) Phishers use the malware purchases to harvest PII, which is then sold to carders. (R3, R4)) Carders then use this PII to make a profit. (B5, B6) As the PII is used multiple times, the profit resulting from each use decreases, as the victim has less monetary assets to obtain.

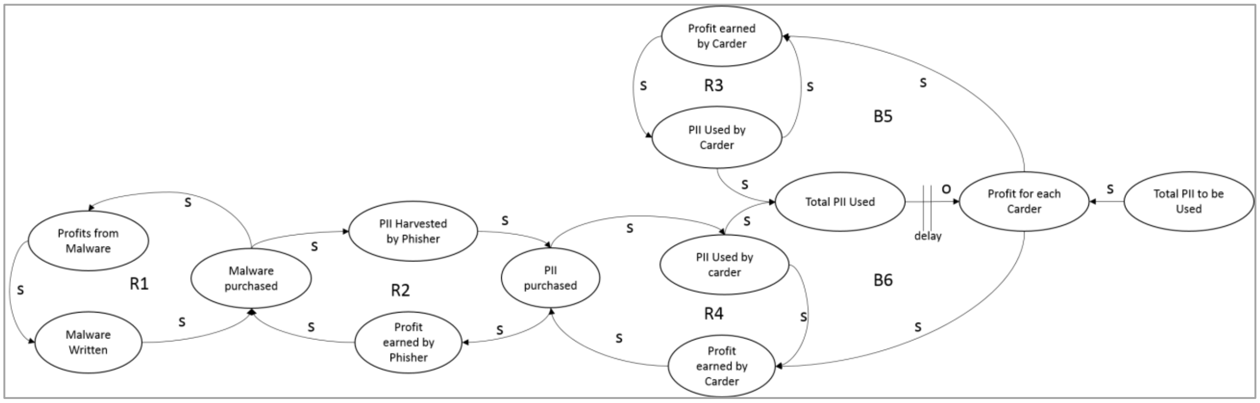

Figure 9 - Causal Loop of Cybercrime Industry

3.2.3.1 Tragedy of the Commons

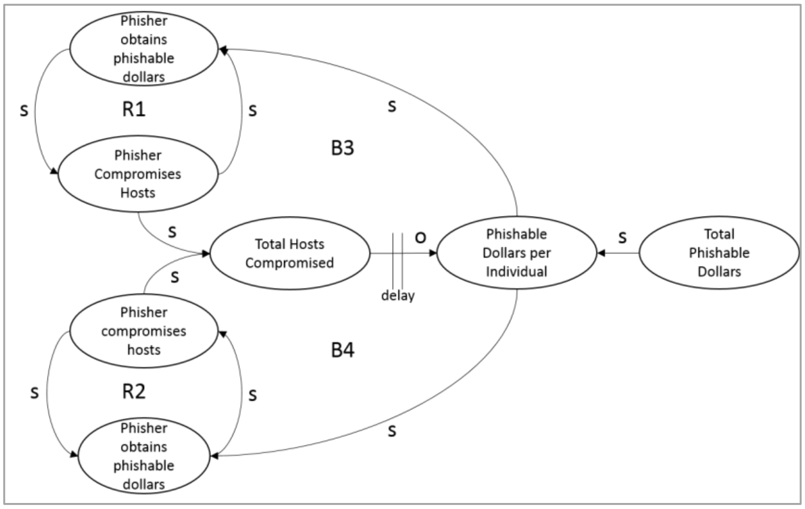
Phisher obtains phishable dollars
s
R1
s
s
B3
Phisher Compromises Hosts
s
Total Hosts Compromised
O
delay
Phishable Dollars per Individual
s
Total Phishable Dollars
s
Phisher compromises hosts
B4
s
R2
s
s
Phisher obtains phishable dollars

Figure 10 – TOC shown for "Phishable Dollars"

Analysis of the causal loop diagram reveals the existence of a system archetype. Namely, we see that the general structure of the "Tragedy of the Commons" (TOC) archetype can be found in the carder's use of PII. This archetype is characterized by individuals increasing their consumption of a common, finite resource both out of reward and out necessity when, eventually, they begin to notice the rewards decreasing. The result of this increased consumption by all parties eventually causes the finite resource to be "significantly depleted, eroded, or entirely used up" (Senge, 1994)[xxxv]. In a report published by Microsoft, the TOC archetype was applied to the finite resource pool of "phishable dollars" by phishers[xxxvi]. A causal loop diagram reproducing the results from Microsoft can be seen in Figure 7. In this diagram, we can see that all phishers are attempting to obtain the most of a finite resource pool ("phishable dollars"). This revenue is allotted by the number of hosts compromised. As more of the “phishable hosts” are compromised, the total amount of available revenue for each phisher is depleted.

However, in the same way, the tragedy of the commons archetype extends through most, if not all, roles of the cybercrime industry. For example, phishers who extract PII from compromised hosts sell the PII to carders, resulting in a profit to the phisher. This profit motivates the phisher to re-sell the PII to a different carder. This is possible due to the isomorphisms to the market for lemons discussed previously. The carders have no way of determining the credibility of the phisher, and cannot know whether or not the data they are given has already been used or will be used by different parties in the future. The carders who initially obtain access to the data can receive a profitable return on their investment. However, as more carders begin to use the common pool of PII obtained by the phisher, the value left in the PII will diminish. As the carders begin to see diminishing returns, they will increase their activity on the shared resource, resulting in even less value.

The model presented in Figure 6 can be extended to show how the TOC archetype is present in almost every specialized role in the industry. For example, authors of malware may choose to pursue a licensing model that allows buyers to license a copy of their software. However, for the malware to be effective, it must be undetected by most (if not all) current anti-virus products. Sites such as VirusTotal[xxxvii] allow both wary users as well as malware authors to check and see how many popular anti-virus software products properly flag the malware as malicious. As malware authors license their software to consumers, there is a higher risk of it being detected by anti-virus software, lowering the value for all people who use the malware. This creates a TOC archetype in that there is a limited number of “undetected

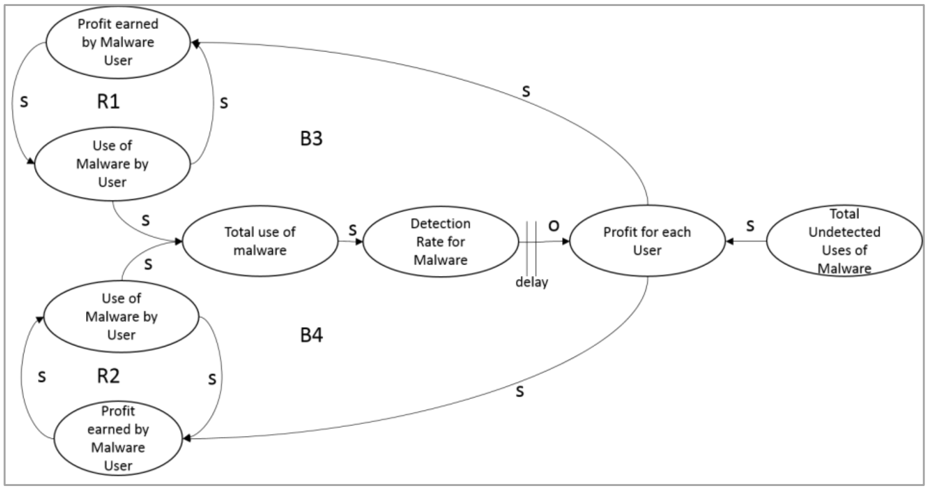
Profit earned by Malware User
s
R1
s
Use of Malware by User
B3
s
s
Total use of malware
s
Detection Rate for Malware
delay
o
Profit for each User
s
Total Undetected Uses of Malware
s
Use of Malware by User
B4
s
R2
s
Profit earned by Malware User
s

Figure 11- Malware TOC archetype

uses” being shared among all purchasers of the malware. The causal loop diagram demonstrating this TOC archetype can be seen in Figure 8.

4. Implications and Points Learned Through Systems Analysis

The isomorphisms that exist between cloud computing and the cybercrime industry can assist researchers in determining the behavior of the industry. By viewing the trends and changes occurring in the cloud computing industry, one can apply the same trends to cybercrime in attempt to discover possible weaknesses in the system before they appear. For example, as hardware and software is becoming cheaper to manufacture and produce, service providers are able scale their operations dramatically, resulting in a decrease in per-instance prices. This same decrease can be observed in botnet hosting. As botnet masters are able to scale their operations into the millions of compromised hosts, discounts can be provided to consumers, resulting in a decrease in per-instance prices.

The isomorphology shared between the cybercrime industry and lemon markets exposes weaknesses in the system behavior which can be exploited by researchers and law enforcement. By introducing intentionally dishonest actors into the system, the already strained trust between sellers and buyers will be replaced by illegitimate business and “fraud against fraudsters”. The cost of this shift will be taken from the cybercrime industry in the form of lost legitimate business and given back to victims through prevented fraud.

In addition, the causal loop analysis shows that, even without intervention by other parties, the system will eventually deplete itself of resources such that cybercrime will not be as profitable as it is now. In fact, the current models show, as reinforced in the report published by Microsoft, that cybercrime may not be as profitable now as current estimations suggest. This future depletion of resources will weaken the system in multiple ways: (1) The lack of profitability of the business will reduce the number of newcomers to the industry, (2) This reduction of newcomers as well as the reduction in the current number of fraudsters will leave fewer actors in the system, (3) It will be easier for law enforcement and financial institutions to monitor, discover, and prosecute the fraudsters.

5. Consideration of the Future Behavior of the System

To complete the systems analysis of the cybercrime industry, it is important to give consideration to the future behavior of the system. Using the isomorphisms and causal loop diagrams constructed previously, we can determine future behavior of this system, and determine the fields of technology cybercriminals are likely to infiltrate next.

5.1 Increase in Mobile Cybercrime

It is estimated that in 2013 there are 6.8 billion cellular subscriptions in use worldwide, resulting in over 95.7% of the global population having access to cellular data. This rise in mobile and, most recently, smartphone use has created the trend of employees performing work related activities on their mobile devices. This trend is called “Bring Your Own Device”, or BYOD[xxxviii]. However, while mobile devices provide a convenient method for workers to perform activities when they are out of the office, these sensitive activities are often performed on open wireless connections which do not provide secure means of communication, passing all traffic (including authentication credentials) as plaintext. In a recent survey performed by GFI, it was discovered that over 99% of employees with a daily commute use their “mobile device for work activities while connected to open public Wi-Fi Internet connections”. The results from this survey, shown in Figure 12, represent a new threat model that is likely to impact businesses and consumers. Criminals are taking notice of the increase in users utilizing smartphone technology, and have already started developing malware designed for mobile devices. The amount of mobile malware is already on the rise, as security firm Kaspersky has detected over 100,000 active mobile malware samples.[xxxix]

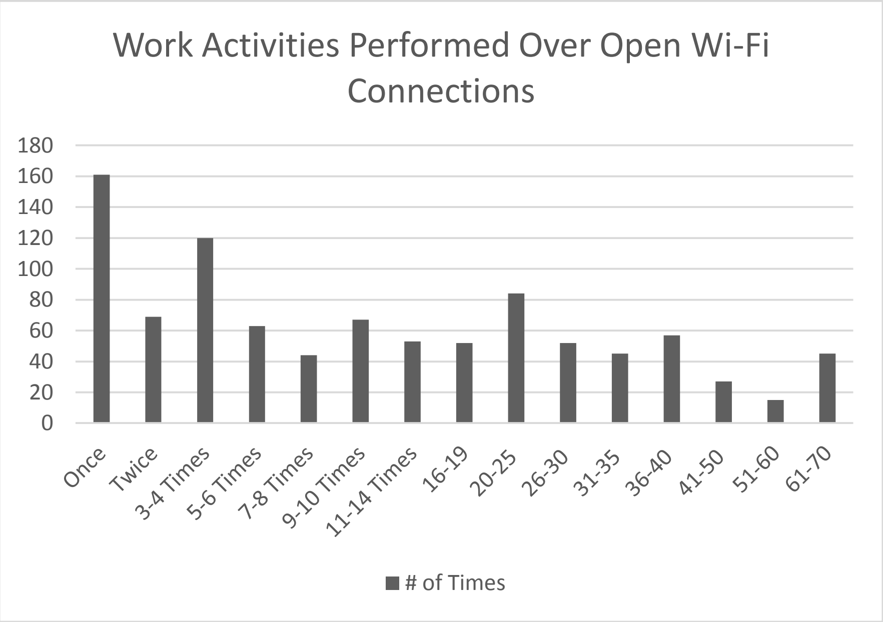

Figure 12 - Work Performed on Open Internet Connections (Source: GFI, 2013)

5.2 Increase in "Internet of Things"

In addition to the increase in mobile devices, the technology industry has also seen in increase in general embedded devices. Devices such as "smart TVs" and home automation systems are driving the industry towards an "Internet of Things", or, "Internet of Everything". It is estimated that, due to the "dramatic increase in processing power, storage, and bandwidth at ever-lower costs", over 50 billion devices will be interconnected by the year 2020 (Cisco, 2013)[xl]. While this is a relatively new trend in technology, by using our previously discovered isomorphisms between the cybercrime industry and cloud computing or technology industries, it can be predicted that cybercriminals will likely find opportunities to perform fraud utilizing these new devices in the near future.

5.3 Reinforcing the TOC Archetype and Equifinality

It is important to consider that these new fields of devices being actively exploited by attackers simply adds to the already finite resources available to attackers. In holding true to the TOC archetype discovered previously, these resources will eventually be depleted and cause a loss in profitability for the cybercrime industry. In fact, it could be regarded that attackers are moving away from the compromise of standard PCs and towards mobile devices because the markets have already been saturated, and the resources have already been depleted. The only impact these additional avenues for attack will have on the existing organizational structure models will be to prolong the inevitable depletion of profit as a whole. The principle of equifinality still holds true in that the system can still reach the same end state regardless of the initial or intervening states. The TOC archetype shows the final depleted and unprofitable state of the system, and adding additional finite resources will not change this final state.

6. Conclusion

It can be observed that, with the recent expansion of the cybercrime industry, traditional techniques can no longer be applied to study the system. However, through the use of general systems techniques, it is possible to study this underground economy as an organismic "whole". Through a systems analysis, it has been observed that the cybercrime industry indeed qualifies as an open-system, and exhibits many of the same characteristics of a system posed by Bertalanffy such as centralization, mechanization, individualization, and segregation (Bertalanffy, 1968). By discovering isomorphisms to similar services and industries, it is possible to study the behavior of the system, as well as potentially predict future behavior. In addition to this, through causal loop analysis it was determined that the cybercrime suffers from multiple instances of the Tragedy of the Commons (TOC) archetype. Since the system is also isomorphic to lemon markets, there are no mechanisms in place to balance out the impending depletion of finite profitability of the system. These weaknesses in the system lead to the conclusion that the system is already not as profitable as existing estimations suggest, and that researchers and law enforcement can further exploit these weaknesses to drive legitimate business out of the market, reducing the impact cyber fraud has on the global economy.

Bibliography

[i] "The World in 2013: ICT Facts and Figures." ITU, 2013. Web. 25 Nov. 2013. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>.

[ii] Akerman, Nick, Ross Anderson, Ph.D., Ashish Arora, Ph.D., Augusto Paes De Barros, Renato Blum, Lynn Carter, Lilian Edwards, Gail F. Farnsely, Marco Gercke, Karthik Kannan, Sivarama Krishnan, Heejo Lee, Tom Longstaff, Ph.D., Jacquelyn Rees, Timothy J. Shimeall, Eugene H. Spafford, Yoshiyasu Takefuji, Ph.D., Katsuya Uchida, Michael Versace, and Sun Yuqing, Ph.D. "Unsecured Economies: Protecting Vital Information." McAfee, 29 Jan. 2009. Web. 9 Nov. 2013. <http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf>.

[iii] "THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE." Mcafee.com. Center for Strategic and International Studies, July 2013. Web. 9 Sept. 2013. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>.

[iv] Totty, Michael. "The First Virus..." The Wall Street Journal, 26 Sept. 2011. Web. 9 Nov. 2013. <http://online.wsj.com/news/articles/SB10001424053111904265504576568770117066288>.

[v] "The Evolution of Cybercrime." *Internet Security, AntiVirus, AntiSpam, AntiSpyware*. McAfee Security Advice Center, Spring 2013. Web. 25 Nov. 2013. <http://home.mcafee.com/advicecenter/?id=rs_na_sp11article1>.

[vi] Herley, Cormac, and Dinei Florencio. "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy." Microsoft, 1 June 2009. Web. 22 Nov. 2013. <http://research.microsoft.com/pubs/80034/nobodysellsgoldforthepriceofsilver.pdf>.

[vii] "REQUEST FOR RECORDS DISPOSITION AUTHORITY." Internet Crime Complaint Center (IC3), 24 Mar. 2011. Web. 25 Nov. 2013. <http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-11-016_sf115.pdf>.

[viii] "About Us." US-CERT. N.p., n.d. Web. 22 Nov. 2013. <http://www.us-cert.gov/about-us>.

[ix] "IFCC 2001 Internet Fraud Report." National White Collar Crime Center and the Federal Bureau of Investigation, 2002. Web. 25 Nov. 2013. <http://www.ic3.gov/media/annualreport/2001_IFCCReport.pdf>.

[x] "EBay." Electronics, Cars, Fashion, Collectibles, Coupons and More Online Shopping. N.p., n.d. Web. 22 Nov. 2013. <http://ebay.com/>.

[xi] "Annual Reports." Internet Crime Complaint Center (IC3). Internet Crime Complaint Center (IC3), n.d. Web. 10 Nov. 2013. <http://www.ic3.gov/media/annualreports.aspx>.

[xii] "Responding to the Financial Cybercrime Epidemic." CyberCrime 2010 Symposium, 4-5 Nov. 2010. Web. 25 Nov. 2013. <http://cybercrime2012symposium.com/assets/CyberCrime2010-Insights.pdf>.

[xiii] Samani, Raj, and Francois Paget. "Cybercrime Exposed: Cybercrime-as-a-Service." McAfee® Labs, n.d. Web. 25 Nov. 2013. <http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf>.

[xiv] "Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002." Office of Management and Budget, 7 Mar. 2012. Web. 25 Nov. 2013. <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf>

[xv] Finkle, Jim. "Hackers Steal U.S. Government, Corporate Data from PCs." *Reuters*. Thomson Reuters, 17 July 2007. Web. 21 Nov. 2013. <http://www.reuters.com/article/2007/07/17/us-internet-attack-idUSN1638118020070717>.

[xvi] Ragan, Steve. "The Tech Herald." *ZBot Data Dump Discovered with over 74,000 FTP Credentials*. The Tech Herald, 29 June 2009. Web. 21 Nov. 2013. <http://www.thetechherald.com/articles/ZBot-data-dump-discovered-with-over-74-000-FTP-credentials/6514/>.

[xvii] "Reversal and Analysis of Zeus and SpyEye Banking Trojans." IOActive Inc., 2012. Web. 25 Nov. 2013. <http://www.ioactive.com/pdfs/ZeusSpyEyeBankingTrojanAnalysis.pdf>.

[xviii] Caballero, Juan, et al. "Measuring Pay-per-Install: The Commoditization of Malware Distribution." USENIX Security Symposium. 2011.

[xix] Zeller, Tom, Jr. "Black Market in Stolen Credit Card Data Thrives on Internet." New York Times, 21 June 2005. Web. 23 Nov. 2013. <http://www.nytimes.com/2005/06/21/technology/21data.html?_r=0>.

[xx] Bertalanffy, Ludwig Von. *General System Theory; Foundations, Development, Applications.* New York: G. Braziller, 1969. Print.

[xxi] Cruz, Benjamin, Paula Greve, Francois Paget, Craig Schmuger, Jimmy Shah, Dan Sommer, Bing Sun, Adam Wosotowsky, and Chong Xu. "McAfee® Labs Threats Report: Third Quarter 2013." McAfee® Labs, 2013. Web. 25 Nov. 2013. <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf>.

[xxii] Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Sept. 2011. Web. 25 Nov. 2013. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

[xxiii] Support, Rackspace. "Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS."*Knowledge Center*. Rackspace, 22 Oct. 2013. Web. 23 Nov. 2013. <http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas>.

[xxiv] Kotov, Vadim, and Fabio Massacci. "Anatomy of Exploit Kits." Engineering Secure Software and Systems. Springer Berlin Heidelberg, 2013. 181-196. <http://cseweb.ucsd.edu/~voelker/pubs/eaas-ccs12.pdf>.

[xxv] Binsalleeh, Hamad, et al. "On the analysis of the zeus botnet crimeware toolkit." Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE, 2010. <http://www.ncfta.ca/papers/On_the_Analysis_of_the_Zeus_Botnet_Crimeware.pdf>.

[xxvi] Howard, Fraser. "Exploring the Blackhole Exploit Kit." SophosLabs, UK, Mar. 2012. Web. 23 Nov. 2013. <http://sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf>.

[xxvii] "SECOND SUPERSEDING INDICTMENT." UNITED STATES OF AMERICA, 2013. Web. 25 Nov. 2013. <http://www.justice.gov/iso/opa/resources/5182013725111217608630.pdf>.

[xxviii] Matrosov, Aleksandr, Eugene Rodionov, Dmitry Volkov, and David Harley. "When You're in a Black Hole, Stop Digging." EMET, n.d. Web. 25 Nov. 2013. <http://www.eset.com/us/resources/white-papers/carberp.pdf>.

[xxix] "Grappling with the ZeroAccess Botnet." *Endpoint, Cloud, Mobile & Virtual Security Solutions*. Symantec, 20 Sept. 2013. Web. 25 Nov. 2013. <http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet>.

[xxx] "Amazon Elastic Compute Cloud (Amazon EC2)." *AWS*. Amazon, 2013. Web. 24 Nov. 2013. <http://aws.amazon.com/ec2/>.

[xxxi] Goncharov, Max. "Russian Underground 101." Trend Micro, 2012. Web. 25 Nov. 2013. <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>.

[xxxii] Samani, Raj, and Francois Paget. "Digital Laundry - An Analysis of Online Currencies, and Their Use in Cybercrime." McAfee® Labs, n.d. Web. 25 Nov. 2013. <http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf>.

[xxxiii] Akerlof, George. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84.3 (1970): 488-500. JSTOR, 27 Aug. 2007. Web. 25 Nov. 2013. <http://www.iei.liu.se/nek/730g83/artiklar/1.328833/AkerlofMarketforLemons.pdf>.

[xxxiv] Herley, Cormac, and Dinei Florencio. "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy." Microsoft, n.d. Web. 25 Nov. 2013. <http://research.microsoft.com/pubs/80034/nobodysellsgoldforthepriceofsilver.pdf>.

[xxxv] Senge, Peter M., The fifth discipline, Currency Doubleday New York (1994).

[xxxvi] Herley, Cormac, and Dinei Florencio. "A Profitless Endeavor: Phishing as Tragedy of the Commons." Microsoft, n.d. Web. 25 Nov. 2013. <http://research.microsoft.com/pubs/74159/PhishingAsTragedy.pdf>.

[xxxvii] "VirusTotal - Free Online Virus, Malware and URL Scanner." *VirusTotal - Free Online Virus, Malware and URL Scanner*. N.p., n.d. Web. 25 Nov. 2013. <https://www.virustotal.com/>.

[xxxviii] "Bring Your Own Device." *The White House*. N.p., n.d. Web. 25 Nov. 2013. <http://www.whitehouse.gov/digitalgov/bring-your-own-device>.

[xxxix] "Antivirus Protection & Internet Security Software." *Kaspersky Lab IT Threat Evolution: Q2 2013*. Kaspersky Lab, 15 Aug. 2013. Web. 25 Nov. 2013. <http://www.kaspersky.com/about/news/virus/2013/kaspersky_lab_it_threat_evolution_q2_2013>.

[xl] Bradley, Joseph, Joel Barbier, and Doug Handler. "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion." Cisco, 2013. Web. 25 Nov. 2013. <http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf>.