Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy

Cormac Herley and Dinei Florêncio
Microsoft Research
One Microsoft Way
Redmond, WA, USA
c.herley@ieee.org, dinei@microsoft.com

ABSTRACT

Much attention has been devoted recently to the underground economy, and in particular to the IRC markets for stolen identities, phishing kits, botnets, and cybercrime related services. It is suggested that sophisticated underground markets show great specialization and maturity. There are complex divisions of labor and service offerings for every need. Stolen credentials are traded in bulk for pennies on the dollar. It is suggested that large sums move on these markets.

We argue that this makes very little sense. Using basic arguments from economics we show that the IRC markets studied represent classic examples of lemon markets. The ever-present rippers who cheat other participants ensure that the market cannot operate effectively. Their presence represents a tax on every transaction. Those who form gangs and alliances avoid this tax, enjoy a lower cost basis and higher profit. This suggests a two tier underground economy where organization is the route to profit. The IRC markets appear to be the lower tier, and are occupied by those without skills or alliances, newcomers, and those who seek to cheat them. The goods offered for sale on these markets are those that are easy to acquire, but hard to monetize. We find that estimates of the size of the IRC markets are enormously exaggerated. Finally, we find that defenders recruit their own opponents by publicizing exaggerated estimates of the rewards of cybercrime. Those so recruited inhabit the lower tier; they produce very little profit, but contribute greatly to the externalities of cybercrime.

1. INTRODUCTION

There has been a recent surge of interest in the underground economy, both in the popular and academic presses. A common theme is the observation that there is a thriving market in the goods and services associated with online crime [27, 17, 3, 4]. Hackers who used to seek exploits for recreation or reputation have given way to those who are in it for the money. For example, an NY Times story "Black Market In Credit Cards Thrives on Web" (June 21, 2005) relates that "The online trade in credit card and bank account numbers, as well as other raw consumer information, is highly structured. There are buyers and sellers, intermediaries and even service industries." The underground economy described, in the NY Times and elsewhere, appears to mirror the real economy in many respects. There are well-defined specializations and complex divisions of labor. For example, some have stolen credentials for sale, while others act as cashiers to drain the accounts. Some develop phishing kits for sale while others maintain compromised hosts on which they can be deployed. Specialization is a usually a sign of developed economies, and generally increases the productivity of labor [7]. Thus the specialization observed is often taken as an indication of the size, maturity and value of the underground economy. There is a considerable and growing body of work documenting the activity on these markets.

While at first glance plausible, the accounts that reach us of this underground economy present a number of facts that do not make sense. First, common to most of the underground economy studies is the observation that stolen credit card numbers (CCNs) and credentials sell for pennies on the dollar. For example, Symantec [4] finds the asking price for a CCN varies between \$0.5 and \$12, even when the available balance is several thousand dollars. Thomas and Martin [27] quote an IRC exchange where 40k financial accounts with face value of \$10 million are valued at less than \$500. This makes very little sense. Why would anyone sell for 50 cents an asset that is worth \$2000? If the seller can't turn the CCN into cash himself surely someone will do it for less than the 99% and higher premiums that these numbers imply.

Second, several of the underground economy studies refer to large numbers of CCNs posted openly on the wire [27, 17, 3, 4]. That is the information is posted for all on the IRC channel to see. Symantec reports finding 44752 individual pieces of personal data, such as SSNs or CCNs, during a year [4]. Franklin *et al.* report a daily average of 465 CCNs posted on the single

IRC channel they monitored. Some suggest that posting stolen CCNs is a way for participants to have their user nics verified [27], while others claim that posting free samples is a mechanism for sellers to attract business [17].

Third, the openness of the underground economy markets would appear to invite counter-measures. That is, if it has been easy for security researchers to find and function on these networks the same should be true of bank employees or law enforcement officials. According to Symantec [4]: "joining is usually open to anyone, often entailing registration with only a username." A bank can easily post honey pot CCNs on the channel to investigate the cash out strategy of hackers. Law enforcement can easily identify cashiers and drops by offering transactions and following the money. Franklin *et al.* [17] suggest a number of simple elegant countermeasures that could even be fatal to the market (see Section 4.1). It simply defies common sense to have a large underground economy that is so easily accessible to all.

Fourth, there is huge variance in the estimates of the amounts of money at stake in the underground economy. Popular press accounts tend to the sensational and talk about billions that trade on the underground economy markets. Symantec tallies the total asking price of all the CCNs they observed offered for sale at $163 million, but estimates the potential worth of those CCNs at $5.3 billion. Gartner puts 2007 phishing losses in the US at $3.2 billion. Yet, in previous work [16] we find that the losses are more likely in the vicinity of $60 million. Kanich *et al.* [20] found that a major spam campaign that involved 350 million emails sent, garnered revenue of only $2731.88. They point out that anecdotal reports of $80 per million for spam delivery would be too expensive by a factor of twenty for this campaign to make sense. Further, the revenue gained involved 75k botnet machines: that's a return of 50 cents per botnet machine per year. Even allowing that a botnet machine could be rented in parallel to do many things we have two orders of magnitude difference between the frequently quoted $1 per botnet machine per day and this measurement. Thus, there are enormous differences between the various estimates of the values of exploits: 32× between the ask and potential value of CCNs, 50× between two phishing estimates, 20× between return on a spam campaign and quoted spam rates, and 100× between the revenue from a botnet and quoted rental rates.

Finally, every account of the underground economy makes reference to rippers [27, 17, 3, 4, 22]. Rippers are participants in IRC markets who do not provide the goods or service for which they've been paid. They are energetic, inventive, and appear everywhere. How is it possible for a market to function when dishonesty is so easy and so profitable?

This paper is an attempt to resolve some of these apparent paradoxes using arguments from Economics. We find that the underground economy IRC markets are a classic example of a market for lemons [13]. That is, there is information asymmetry between buyer and seller: the uncertainty for a buyer in knowing whether he is dealing with a ripper or not. Every account we have of the underground economy makes clear that rippers are a real and ever-present menace. This uncertainty causes adverse selection, where rippers are attracted to the market (since they get money for nothing), while legitimate sellers tend to stay away (since the probability of getting ripped off is factored into everyone's buying decisions). Unchecked this causes the market to fail [13].

Essentially the risk of dealing with a ripper represents a tax on every transaction conducted in the market. Those who can avoid this tax have lower costs and higher profits; and the simplest way of avoiding the tax is to form deals repeatedly with partners who perform. It makes no sense to transact with anonymous market participants when there is considerable quality uncertainty *unless there is no alternative.*

This has a number of implications for the underground economy. While there is a great deal of activity in the underground economy market place, it does not imply a lot of dollars change hands. The important deals happen where the ripper tax cannot reach them. This means that the IRC markets are a very low-value channel. We believe that anyone who shows up on an IRC channel hoping to trade profitably with anonymous partners is almost certain to be cheated. Thus, estimating the dollar size of the underground economy based on the asking price of good and services advertised on IRC networks appears unsound. Finally, the presence of a ripper tax on IRC channels points to a two tier system in the underground economy: those who are members of alliances and gangs remove a major cost from their business. Those who trade on IRC channels do so because they have no choice, or they are seeking to cheat. Thus, far from being a sophisticated clearing house where professional criminals trade specialties the IRC channels appear to be the bottom rung, where those with few skills, connections or experience mix with rippers.

2. RELATED WORK

2.1 Studies of the Underground Economy

Thomas and Martin [27] were among the first to draw attention to and document the growing activity in the underground economy. They found enormous activity on IRC channels advertising stolen goods and services such as phishing kits, credentials *etc.* They colorfully describe the underground economy as an extremely

busy market-place where individuals who specialize in particular activities trade goods and services to others. Some will produce phishing kits, some will offer hosting services, some sell credentials and still others offer to cash-out the actual dollars from compromised accounts. Abad [8] also offers an early view of the underground ecosystem that supports phishing. Franklin *et al.* [17] followed with a very detailed measurement study of an IRC market, and document the activity in a principled way. For example they found over 100k active user accounts on a single IRC trading channel, and measured an enormous quantity of credentials and services offered for sale.

Symantec has produced a series of reports on Internet Security and the underground economy. They appear to corroborate the view that the market for goods and services related to stolen credentials has become big business [3]: "The emergence of underground economy servers as the de facto trading place for illicit information is indicative of the increased professionalization and commercialization of malicious activities over the past several years." In 2008 Symantec [4] finds that stolen credit cards are selling for as little as $0.10, but that the potential worth of all the credit cards was $5.3 billion: "Cybercrooks have developed sophisticated business models such that recognized job roles and specialisms have evolved in the 'recession proof' digital underground."

Geer and Conway [9, 10] informally suggest an Øwned Price Index of underground economy asking prices to track changes in the markets.

Dhanjani and Rios [22] also investigate an IRC marketplace and also observe impressive activity. Interestingly they find that phishers prey on each other: phishing kits offered for sale in the market turn out to have obfuscated backdoor code that reports the details of any credentials harvested to the author as well as to any user of the kit. Among their interesting observations are that many participants are unsophisticated and inexperienced, and a great many phishers struggle to monetize their exploits. Cova *et al.* [21] also observe obfuscated backdoors in phishing kits available on these markets.

Zhuge *et al.* [18] carry out a study on the Chinese underground economy, again focussing on activity and advertisements. The IRC channels popular elsewhere are less used in China.

Kanich [20] managed to invade a spamming botnet and track the amount of spam sent, the transactions conducted and the dollars that appear to have changed hands. They observe that in a 26 day study of a spamming botnet 350 million emails resulted in only 28 sales and total revenue of $2731.88. Interestingly, they suggest that the spam services they studied are produced by the controllers of the botnet itself. This suggests that the service is entirely integrated rather than sold as a commodity service to others (see Section 4.3).

John *et al.* [19] also provide a very detailed study of a spamming botnet. They find, for example, that a small number of botnets account for a majority of spam. This corroborates the view that a few well organized gangs dominate the space.

Holz *et al.* [31] carry out a study of dropzones (*i.e.* servers that are used to park stolen credentials). They observe the number of stolen credentials that get stored, but have no direct means of estimating the value of each. They take the Symantec [3] estimates of the value of credentials to arrive at a figure for the size of the underground economy they study.

2.2 Economics of Security and of the Underground Economy

Anderson [25] first proposed the comprehensive examination of security from an Economics perspective, and developed on the theme with others [26]. They observe, for example, that economists have long studied how misaligned incentives produce undesired outcomes, and many of these results carry lessons for security. The study of negative externalities, where economic actors do not bear the full cost of their actions also has great applicability in network and internet security.

Since 2001, the Workshop on the Economics of Information Security has explored these and other areas of overlap between economics and security. For example, there has been much interesting work on the establishment of a market for security vulnerabilities [6] and the economics of privacy [5].

Many works have studied the economics and mechanisms that govern the behavior of the "good guys" and study how things can be made better. There has also been examination of the economics and mechanisms that govern the behavior of the "bad guys" and study how things can be made worse. Fultz and Grosslags [23] examine the case where, like the defenders, attackers are in a resource constrained environment. When there are too many of them, all seeking easy returns, yield falls. Two related papers propose to insert uncertainty in the botnet infrastructure, with the objective of increasing uncertainty in the service provided by the botnets, thus reducing its value. Ford and Gordon [12] propose that once a machine is recovered from a botnet, instead of letting the botnet master know, we maintain association with the botnet, and even increase the click/display rate. This would increase the uncertainty, reducing the value of the service provided by adware. Li *et al.* [32] propose increasing uncertainty in the botnet economy by setting up honeypots and allowing them to infiltrate the botnet environment, increasing uncertainty in how many machines a botnet really has available for a denial of service attack.

In an earlier work we examined the economics of phishing [16]. We found that phishing is a classic example of Tragedy of the Commons where open access to a shared resource drives the total returns down. One of our surprising findings was that total *direct* dollar losses from phishing appear to be far lower than generally thought. However, this fits neatly with the notion of security as an externality [26]: the direct dollar losses are far from being a complete accounting of the problem. We explore that question further in Section 4.6.

2.3 Economics Background

2.3.1 Asymmetric Information: The Market for Lemons

In a classic paper, Akerlof [13] examined the effect of uncertainty on markets. In a situation where sellers have better information than buyers about the quality of their wares there is adverse selection and the "bad drive out the good." Choosing the specific example of used cars where the seller knows whether the car is a lemon or not the buyer will logically factor the average likelihood of getting a lemon into the price. Thus sellers of good cars get less than their cars are worth, while sellers of lemons get more. This leads to adverse selection where sellers of lemons are attracted to the market, while sellers of good cars tend to stay away. This increases the percent of lemons in the market driving the average quality further down.

Where there is a continuum of quality the problem can lead to a market failure. Suppose a product has quality q uniformly distributed in the range $[0, 1]$. Suppose that for every q there are sellers who are willing to sell their product for any price above q, and buyers who are willing to buy for any price below $3q/2$. The price would then achieve equilibrium at some point between q and $3q/2$ if quality were observable. However, since the seller knows the quality while the buyer does not, the buyer can only decide his price based on the average or expected quality. At any possible equilibrium price p, only products in the quality range $[0, p]$ will be offered for sale, so that the average quality is $p/2$. However buyers will pay only $3p/4$, for a product of expected quality $p/2$ and thus no trades happen.

What is interesting is that even though willing buyers and willing sellers exist for products at every quality in the range $[0, 1]$ no trades happen. There are buyers who would happily pay $3q/2$ for a products of quality q and sellers who will take this price. But the buyer has no way of verifying that the product is really of the claimed quality, and the seller has no way of credibly disclosing q. A lemon market will be produced by the following:

- Asymmetry of information, in which no buyers can accurately assess the value of a product through examination before sale is made and all sellers can more accurately assess the value of a product prior to sale
- An incentive exists for the seller to pass off a low quality product as a higher quality one
- Sellers have no credible quality disclosure technology
- Either there exist a continuum of seller qualities or the average seller type is sufficiently low
- Deficiency of effective public quality assurances (by reputation or regulation and/or of effective guarantees / warranties)

Akerlof suggested that lemon Markets existed in the market for used cars, the insurance and job markets, and in the market for debt in underdeveloped economies.

The claim that security products are a market for lemons has been noted [25]. That is the buyer often has a poor understanding of the risk mitigated and the protection gained, and is poorly equipped to make an informed distinction between a good security product and a bad one. Grigg argues that security products are actually a market for silver bullets [1] since neither buyer nor seller actually understands the risks. While it is interesting that the market for lemon theory has been applied to security goods before, the argument we advance is quite different. We argue that several of the goods traded in the underground economy satisfy the criteria for a market for lemons.

2.3.2 The Theory of the Firm

A subject of great interest in economics is the theory of the firm. That is, why do firms exist instead of letting the market decide all prices. For example, why does it make sense for a company to have long term employees rather than purchase labor as needed in the market.

Coase [28] advanced the transaction cost theory of the firm in 1937. When the transaction costs are high or uncertain it is advantageous to form firms.

3. THE UNDERGROUND ECONOMY IS A MARKET FOR LEMONS

As discussed in Section 2.3.1, there are a number of factors that lead to a market for lemons. That there is an incentive to inflate quality claims requires no demonstration. We now go through each of the other criteria in turn and demonstrate that they hold for the goods and services offered for sale in the underground economy.

3.1 The Types of Goods and Services Offered for Sale on the Underground Economy

3.1.1 Goods

Thomas and Martin [27] mention the following goods being advertised on the IRC channel they monitored: CCNs, credentials, scam (phishing) kits and compromised hosts. Franklin *et al.* [17] on a similar channel mention the most common goods being "online credentials such as bank logins and PayPal accounts, sensitive data such as credit cards and SSNs, compromised machines, spamming tools including mailing lists and open mail relays, and scam webpages used for phishing."

Symantec in 2008 [4] tabulates the goods and services offered for sale, which we reproduce in Table 1. The dominance of CCNs is borne out by Thomas and Martin, Franklin *et al.*, Dhanjani and Rios [27, 17, 22].

3.1.2 Services

Thomas and Martin [27] refer to cashiers and drops as the most sought after services in the underground economy. According to Franklin *et al.* the "most common service ad are offers for the services of a cashier, a miscreant who converts financial accounts to cash" [17]. They also find that Confirmers (who answer confirmation questions on the phone) are requested. They find "a small percentage of service ads offer services such as DoS attacks, sending phishing emails, and purchasing goods with other's credit cards (a.k.a., carding)." Other services include drops (physical locations where goods can be sent). Again these findings accord well with those of Symantec as shown in Table 1.

3.2 Is this a Market for Lemons?

3.2.1 Asymmetry of Information

Why does the seller have better information than the buyer as to the value or quality of a set of credentials, CCN, *etc*? First and foremost, the seller knows whether he is a ripper or not. This effect probably dwarves all others.

In addition the most common goods offered for sale on the underground economy are information goods, where quality is hard to determine. The seller knows the balance or available credit limit in the account, while the buyer does not. Also, recall that the buyer requires not merely access to the information, but *exclusive access to the information*. Take for example the stolen credentials for an account with balance $2000. They seller knows the balance, while the buyer must take his word for it (until he gets the password). The value to the buyer might be the full account balance if the buyer can successfully drain the account completely. But this is only possible *if he is the only person attempting to do so*. Nothing prevents the seller selling the same information many times over. If the same credential is sold multiple times each buyer will be competing against an unknown number of would-be harvesters and the return that he can expect changes drastically. The same is true of CCNs and login credentials.

For any type of software application (*e.g.* scam phishing kits, keyloggers *etc*) the situation is even worse: the buyer has no way of determining quality. Anyone who purchases an application runs the risk that it carries an unannounced malicious payload. Phishing kits and keyloggers traded on the underground economy have been found to contain concealed backdoors that remit any information harvested to the author [22, 21]. Again the buyer risks putting himself in competition for the credentials he harvests with others.

Even when dishonesty is not involved some goods have unobservable quality. Mailers and proxies, for example, have useful lifetime related to how much they have previously been used. A phisher who buys an email list and mailer tool to advertise a phishing attempt on PayPal will clearly have lower yield if the same list and tool have been used to advertise several other PayPal phishing sites that week. Proxies that have been extensively used are much more likely to find their way onto blacklists.

Each of these exploits is a question of degree. Of course a ripper also has the simple recourse of entirely failing to deliver once payment is received. For the services traded on the underground economy the uncertainty is whether the seller will perform as advertised. A cashier can fail to hand over the proceeds of a transaction and keep 100% for himself. And a drop can fail to hand over the delivered merchandize.

3.2.2 No credible disclosure

In addition to having better quality information than the buyer the seller has no credible way of disclosing this information to the buyer. A seller who does not intend to cheat, merely subsidizes those who do. Attempts to disclose quality are referred to in several of the studies available. For example (from [27]): "One miscreant even provided a screen shot of a compromised Wells Fargo account, with a net total of US $21,431.18 in cash." However it is difficult to see what assurance this offers: altering the account balance on a screenshot hardly represents a challenge.

Even in the case where the seller offers the buyer a chance to verify the account balance this does not help much. The only thing the buyer can do to guarantee exclusive access is to immediately change the password (and password reset mechanisms) of the account. This might seem an attractive way of excluding any others from the account. This is not feasible however, as for most financial account this generates an email to the user informing them that the password or other information has changed.

The same is true for the services offered. A cashier who will drain an account and remit the proceeds has no credible way of disclosing whether he will perform

Good or Service	Percent of offerings	Asking price range
Bank account credentials	18%	$10-$1000
Credit Card Numbers (with CCV2)	16%	$0.50-$12
Credit Cards	13%	$0.1-$25
Email addresses	6%	$0.30/MB - $40/MB
Email passwords	6%	$4 - $30
Full identities	6%	$0.90 - $25
Cashout Services	5%	8%-50% of total value
Proxies	4%	$0.30 - $20
Scams	3%	$2.5-$100/week for hosting
Mailers	3%	$1-$25

Table 1: Goods and services offered for sale on an underground economy IRC market [4].

honestly or not.

3.2.3 *Continuum of Seller Quality or Low Seller Quality*

The evidence certainly indicates that the average seller quality in the underground economy is extremely low, and cheating and dishonesty are rampant. Thomas and Martin [27] introduce us to the term ripper: a market participant who does not provide the goods or services he's been paid for. This phenomenon appears to be widespread. For example, Franklin *et al.* document a daily average of 490 credit card numbers being posted on an IRC market; however fully 22% of them failed to satisfy the Luhn checksum (*i.e.* they are no better than random 16-digit numbers). They also find evidence that various services offered by the administrator of the channel they monitored were designed to trick participants. For example, commands that check the validity, credit limit and validation number of credit cards were available: !chk, !cclimit and !cvv2. However they did not function as advertised, leading to the suggestion that they are merely a simple way for the channel administrator to steal CCNs from participants. Similarly, Dhanjani and Rios [22] demonstrate the backdoors that some phishers insert in kits so that they can harvest the fruits of other phishers' labor.

Symantec (see Figure 1 of [4]) show a screenshot of a IRC channel with six messages, two of which end with the line "Ripper #$&̂ off" and one of which (for a cashier) promises "you can trust me 100%." Symantec also reports that "Many underground economy servers have channels specifically created by the server administrators as a direct forum to report and list current rippers to avoid. Repeat rippers can be kicked off and banned from the servers." Clearly cheating and dishonesty are a way of life on the underground economy markets, making average seller quality low. Since there is no barrier to entry, it is difficult to imagine a mechanism that would keep seller quality high.

3.2.4 *Lack of Quality Assurance or Regulation*

There are several ways to ensure the functioning of a market in the presence of quality uncertainty. Lemon laws, product warranties, and return policies are efforts to protect the buyer against a bad transaction. However, this clearly works only when there is an enforcement mechanism; and (according to [4]) "In the underground economy, buyers have no recourse to obtain refunds for unsatisfactory goods or services." Further, e-gold, the predominant payment mechanism in the underground economy, promises anonymous irreversible transactions.

The natural way to combat this is to establish a seller reputation mechanism. Indeed even legitimate markets such as eBay require a reputation system to function well. However the reputation system referred to by [27, 17, 3, 4] is very basic: "To establish a reputation and prove themselves, potential sellers are often required to provide samples of their goods for validation and verification." Usernames (nics) are either verified or unverified, and there is no reference to a more complex seller reputation system. In fact the dedicated channels to report rippers appear the only central reputation system. And (as [4] points out): "if an advertiser is accused of being a ripper, he or she can simply switch nicknames and start anew."

Of course individual sellers may perform honestly. But in the absence of a trustworthy seller reputation system this information is diffused among many buyers. Performing honestly in a transaction will effect his reputation with a single buyer, but does not impact his overall reputation in the market. Further, the fluidity with which IRC channels set up and shut down makes complex reputation systems difficult. In addition, as Franklin *et al.* point out a simple slander attack on the reputation of a good seller is not merely possible but profitable for rippers: in assailing good reputation they can drive other sellers from the market and decrease the disadvantage caused by their own lack of reputation [17].

3.2.5 *Summary*

Thus we conclude that each of the goods and services traded on the underground economy indeed satisfy the conditions for a market for lemons. Indeed they satisfy the criteria more faithfully than used cars, since with cars quality is not entirely unobservable, and reputation and enforcement mechanisms do exist. In each of the goods and services offered for sale in the underground economy we find that dishonesty and misrepresentation is not merely possible, but is actually observed and appears very frequent.

Alternatively, suppose not. Suppose the underground economy does not operate as a lemon market and every seller is honest. In this functioning market a single participant who is willing to cheat has an endlessly profitable opportunity.

4. ANALYSIS AND IMPLICATIONS

4.1 Countermeasures ought to be easy: lemonizing the market

The idea of inducing market failure by increasing the quality uncertainty in the market is suggested by Franklin *et al.*[17]. They suggest counter-measures which involve generating many sybil accounts, achieving verified status for each of them, and then conducting deceptive sales. The last step involves offering no-value goods for sale at the market. For example, suppose CCNs are sold at the market at a going rate of $1.25. This may be because the sellers acquisition cost is, say $1.00, and the buyer is able to collect $1.50 on average from each account. Suppose further, there are about 1000 CCNs offered for sale each day on a certain IRC channel. By simply offering another 1000 worthless CCNs for sale, we reduce the expected value per card to $0.75. Since that is below the acquisition cost of the seller, no trade would take place at all even though willing buyers and sellers are both present. It is worth differentiating the above from a Denial of Service attack which would involve bombarding the market. Here just a handful of messages would be enough to cause failure.

This attack makes a great deal of sense. However, as Section 3 shows, the dishonesty and greed of the participants require little encouragement or assistance. They can and do lie, steal and cheat. They are already performing all of the actions that Franklin *et al.* suggest as counter-measures. Thus the underground economy satisfies requirements for a market for lemons, and the counter-measures to attack it appear to be already extensively practised by the market participants themselves.

4.2 The Ripper Tax

In effect, the uncertainty created by the presence of rippers imposes a tax on every transaction conducted in the market. Suppose, for a buyer there is a probability q that a transaction is with a ripper, and $1 - q$ that it is with a legitimate seller. Thus a fraction q of all transactions result in money leaving the system without goods or services changing hands, much as happens with a tax.

It is natural to wonder whether we can estimate the tax rate q. Since none of the underground economy studies [27, 17, 3, 4] observe even a single transaction closing we clearly cannot estimate the fraction of trades where one party is a ripper. However, basic economics and the asking price of goods on the underground economy both suggest that the tax rate is high. First, when a single agency, like a government, applies a tax their goal is to maximize the total tax receipts from the market. If it taxes too heavily activity drops and the return falls. However, the ripper tax is a result of many independent actors each seeking to maximize his personal return. Thus there is a Tragedy of the Commons [15]: rather than show restraint and nurture their collective resource each ripper maximizes his independent profit. The result is a higher tax rate, but lower overall return than the profit maximizing rate [14]. This suggests that rippers drive the tax rate q as high as they can without extinguishing the market entirely. Second, the gap between the asking price for a CCN and its expected fraud value (*e.g.*, $350 according to an FTC victim survey [11]) is due to banks successfully detecting fraud, the premium that the buyer demands to ensure a profit and the ripper tax. The size of the gap suggests the ripper tax must be large.

For example, if banks successfully prevent 90% of fraudulent activity the expected value of a CCN would be $35 rather than $350. To choose a round number let's take $3.50 as a selling price from the range given by Symantec [4]. In a pool of CCNs for sale, a fraction $1 - q$ are good, and q are offered by rippers. A buyer pays $3.50 for CCNs and commits fraud worth $35 on the fraction q of them that are good. Thus, if the buyer demands a 100% premium (*i.e.*, that he double his investment) to make the risk worthwhile, we get $\$35 \times (1 - q) - 3.5 = 3.5$, giving $q = 0.8$. Thus, CCNs sell for $3.50, but 80% of those are offered by rippers. If we consider 1000 CCNs sold then sellers will get $\$3.5 \times 200 = \$700$. Buyers get $\$35 \times 200 - 3.5 \times 1000 = \$3500$. Rippers get $\$3.5 \times 800 = \$2800$.

4.3 Formation of firms and alliances

Taxation of a market is one of the circumstances that Coase [28] identifies as leading to the formation of relationships and ultimately firms. The idea is that when market transactions are taxed, expensive, or uncertain it makes sense to form groups who deal with each other regularly rather than return to the market for every resource requirement. We can readily see how this happens in the underground economy. After a transaction

with a good seller it makes sense to deal with that seller again rather than brave the mixed pool of sellers and rippers. Thus, dealing with someone successfully increases the likelihood that one will deal with them again, since doing so eliminates the ripper tax from the transaction. This is corroborated by each of the studies of the underground economy. For example, Thomas and Martin find [27]: "Those who provide services in the underground economy are looking for long-term customers." Similarly Franklin *et al.* and Symantec find the desire to form partnerships is strong.

There is some evidence that integrated gangs, rather than individuals, are responsible for much online crime. In phishing, for example, the Rockphish gang has been credited with perpetrating about 50% of all attacks [30]. Moore and Clayton find that their attacks are better organized and harder to measure. In examining a large spam campaign launched from the Storm botnet Kanich *et al.*[20] find evidence that the spam is sent on behalf of the botnet controllers, rather than sent as a service for a fee. First, the return is very low, indicating that the service could not be profitably rented for the quoted asking prices. Second, similarity between email addresses used in propagating the botnet and the spam campaign suggests the same people are behind both. Further evidence is given by the concentration of exploits in certain countries and in certain language groups. Four well organized Russian and Ukranian gangs appear to be behind much botherding and spam campaigns [2].

4.4 A Two Tier Underground Economy

The argument we have advanced suggests a two tier system where those who are organized avoid the ripper tax, while those who frequent the IRC channels have higher costs and lower profitability. As the better organized competitors with lower costs those in the upper tier probably enjoy the bulk of the profits. That is, those who see a good return on their investment of time probably belong to gangs that form integrated chains to extract all of the value from their product without having to frequent markets where there is a risk of rippers.

It would also appear that entering the upper tier requires performing as a profitable partner to existing members of the upper tier. Thus, those who possess only commodity skills are unlikely to enter. It is hard to see why an existing alliance or gang in the upper tier would share profits for goods or services that are easily acquired. Upper tier gangs will extract all the value from any resources they control. Thus, as in other spheres, those with few skills who arrive in the underground economy are relegated to the low paying margins. If they succeed in harvesting CCNs or credentials they must sell in ripper infested markets. Further, since they compete with better organized competitors who have a lower cost basis, it appears likely that those who trade on the IRC channels struggle with profitability.

We have argued elsewhere that US phishing losses are about $60 million annually [16]. However, it is probable that the bulk of this gain is concentrated in the hands of the upper tier, while the lower tier makes only their opportunity costs. Levitt and Venkatesh [29] suggest that drug dealing is modelled as a tournament, where participants accept low-pay and high-risk for a small chance of large reward. It is interesting to wonder whether a similar phenomenon might not be at work here. We explore this further in Section 4.6.

4.5 What can we estimate from activity on IRC markets?

4.5.1 What Can We Say about Participants in a Lemon Market?

So why then does the market exist at all? Why does anyone offer goods for sale when they have no way of differentiating themselves from rippers? Even if commerce on IRC channels is taxed, there are various reasons why people will continue to participate in the market:

1. They need to form relationships (with a view to avoiding the ripper tax)
2. They are newcomers and are trying to get started
3. They wish to sell resources that have no value to them
4. They intend to cheat others (*i.e.* they are rippers).

First, while the underground economy servers may represent a dis-functional market it may also be the only way to get required goods or services. For many with criminal services to buy or sell, this is simply the gathering place to meet others with whom one can form mutually beneficial relations. There may be no alternative to a few unprofitable transactions with rippers to find partners with whom one can deal profitably on an ongoing basis. Second, for newcomers this looks like a particularly dangerous place, but they may know no better and have little choice. It appears that offers to help almost universally end up being an attempt to cheat or profit from the newcomer [22, 21]. Third, it certainly makes sense that participants will sell goods or services that they are unable to monetize. For example, if one has CCNs or stolen credentials that one is unable to extract value from, it makes sense to sell them to those who can, even if much revenue is stolen on the way. Also, those who have tried spamming or phishing and found it unprofitable may find it easier to sell services to others who have yet to reach that conclusion [16]. Finally, for rippers the IRC markets appear an ideal playground. But life is competitive, even for rippers: the Tragedy of the Commons [15] again suggests

that rippers will overgraze the underground economy markets and drive overall returns down. The laws of economics haven't been suspended: not for those who steal, nor for those who steal from those who steal.

4.5.2 Activity does not imply dollars

Most of the publicly available data on the underground economy documents activity [8, 27, 17, 10, 4]. It is almost universal to take this as a evidence of profit. We argue that this is profoundly in error. One cannot estimate the gold in the mountains from the activity at the shovel store. In none of the studies of the underground economy do we have examples of transactions actually closing. For legal, ethical and logistical reasons there is not a single confirmed instance of a sale of illicit goods documented in [8, 27, 17, 3, 4].

Symantec [3, 4] uses measured activity to estimate the size of the underground economy. It reports the total asking price of goods offered for sale on all the IRC servers it monitored as $276 million. Of this 59%, or $163 million was CCN related. They then estimate the potential value of these CCNs as $5.3 billion, by assuming that each card suffers the median CCN fraud loss of $350 [11] rather than the $0.50 to $12 for which they are offered for sale. There are a number of problems with this approach.

First, offered for sale does not mean sold. We have no data on what percent of goods offered for sale get sold. Recall the spam campaign which achieved 27 sales for 350 million emails sent [20]. Indeed, if we applied the assumption that everything advertised was sold, we would conclude that that campaign would have yielded $8.75 billion rather than the $2731 actually achieved: a difference of six orders of magnitude! Second, asking price in a market riddled with dishonesty isn't necessarily an accurate indication of what the goods are worth. Taking the average of unverified numbers creates great opportunity for upward bias. Those who ask high prices and sell least affect the average most. More significantly, taking the average of offered sales includes the worthless goods offered by rippers. Finally, assuming that each offered-for-sale CCN results in $350 worth of fraud, rather than the $0.5 to $12 range for which it was offered seems unrealistic. This assumes that banks detect no fraud, and assumes that sellers allow others to extract more than 95% of the value of their product. While this is possible, a simpler explanation would be that CCNs are offered for $0.50 to $12 because, in expectation, they are worth no more than a small multiple of that (to account for the profit margin) to the buyer.

Returning to the $163 million worth of CCNs that Symantec observed: if we assume that only a quarter of what is offered actually sells, and that buyers achieve a 100% premium (*i.e.*, double their at-risk money) we get a value of $82 million rather than the $5.3 billion. This is a high estimate of the total fraud from all of the CCNs that Symantec observed offered for sale: it's doubtful that even a quarter of offered goods get sold.

The history of any goldrush reminds us that effort does not imply reward. For example, over 100000 prospectors attempted to reach the Klondike after gold was discovered in 1897 [24]. Of these fewer than 4000 actually found any gold, and a few hundred found enough to cover their costs and perhaps get rich. The total value of the gold extracted from the Klondike is estimated at $50 million, while the average prospector spent $1000 and Seattle merchants alone sold over $25 million worth of goods to those heading to the gold fields [24].

4.5.3 Activity does imply Competition

Even if we cannot estimate the dollar size of the merchandise traded on IRC markets there is a great deal we can learn from the amount of activity. First, this is an extremely competitive market. There is enormous activity from those seeking riches.

Second, there is a lot of cheating. This can itself be taken as evidence that many find the underground economy a very challenging environment. Newcomers are beset by offers of kits, tutorials and gear [4] much as those going to the Klondike were offered merchandize from those who preferred to trade than try their luck in the gold fields [24]. The extent to which cheating and rippers are a factor suggests that life in the underground economy is not as easy as it is often portrayed. If getting credentials and draining accounts worth thousands of dollars were simple why would anyone waste their time ripping by, *e.g.*, offering to sell non-existent CCNs for $0.50 each? This evidence suggests that rippers are better informed than their victims about the returns on exploits such as phishing and spam.

4.5.4 What can we say about the goods offered in a Lemon Market?

We argue in Section 4.5.2 that activity cannot be used to estimate the dollar size of the underground economy. But we can still learn much of its workings by observing activity. Anyone who chooses to buy or sell in a heavily taxed market clearly has few other options. The fact that he pays the ripper tax tells us that he has little alternative. For a seller this means that he cannot monetize the goods himself, and does not have access to someone who can do so for a smaller premium than the ripper tax. This suggests that the goods and services advertised on the underground economy are those that are easy to acquire, but hard to monetize.

4.6 Who are we Fighting? What are we Trying to Accomplish?

The picture that emerges is of a two tier underground economy where the inhabitants of the lower tier are

taxed by rippers and struggle to monetize their efforts. Why does this matter? If all we cared about were the direct losses from cybercrime it might not be important. Why should we care if one subset of cybercriminals get cheated by another? However, the gains enjoyed by participants in the underground economy are not an accurate measure of the size of the problem. For example, Kanich *et al.* show that a 350 million email campaign resulted in a mere $2731 in revenue for the spammer. Clearly, this gain is minor in comparison to the externalities: the value of the infrastructure required to handle and store this email, the spam filtering work required, and the time wasted by recipients. A similar pattern holds with other forms of cybercrime.

While the inhabitants of the lower tier struggle to monetize their efforts it does not follow that they account for a small portion of the externalities. For example, the bulk of the profits from phishing may be concentrated in the hands of a few gangs, but responsibility for the erosion of trust, cost of customer support calls, and expense of educating users and deploying stronger authentication mechanisms belong to all those who phish, not just those who make a profit. Consider two different phishers. An upper tier phisher who gets 100 credentials per million emails delivered into inboxes, and a lower tier phisher who gets one credential per million emails delivered. The contributions of these two to the direct costs of phishing are very different, while their contributions to the externalities are similar. This brings us to the important questions of who we are fighting and what we are trying to accomplish.

Who are we fighting? Those in the upper tier are engaged in a profitable activity, and are members of alliances or gangs. It is reasonable to expect that they will respond to economic and law enforcement pressures much as any other firm will. However, those in the lower tier appear to struggle with profitability. We can explain their persistence using the tournament model of the job market that Levitt and Venkatesh [29] apply to the drug trade. Newcomers accept low pay and high risk in exchange for a chance of a large reward.

What are we trying to accomplish? If we cared only about direct losses we would concentrate on the upper tier. We could effectively ignore the lower tier, since they gain little for their efforts. However, the evidence from spam [20] and phishing [16] is that the direct losses are minor compared to the externalities. To reduce the externalities we must fight both upper and lower tiers. In fact, the numerically greater lower tier probably accounts for the bulk of the externalities.

Unfortunately, if the lower tier is largely unprofitable, and acts as a tournament job market it may be relatively impervious to economic and law enforcement pressures. Participants are striving for their chance at reward and are willing to endure difficulties, risk and loss. Thus the tools that the upper tier responds to have less influence on the lower tier. However, this does suggest a third approach: if lower tier participants are misinformed about the true likelihood of winning, *i.e.*, overestimate the rewards, then it may be possible to influence them by publicizing accurate information. That is, as those who are new and inexperienced, lower tier participants believe that the underground economy is a path to easy riches. Where do they get that idea? From the same place the rest of us get that idea: unreliable and exaggerated estimates repeated without scrutiny. We suggest that accurate estimates are not just interesting from a research standpoint, but can have material influence on the recruitment of our opponents.

5. CONCLUSION

The underground economy is often painted as an easy money criminal Utopia where even those without skills can buy what they need and sell what they produce. They can buy phishing kits, rent hosting services and then profitably sell the credentials they produce on IRC channels. This picture does not withstand scrutiny. The IRC markets on the underground economy represent a classic example of a market for lemons. The rippers who steal from other participants ensure that buying and selling is heavily taxed.

Avoiding the ripper tax reduces costs and increases profitability. Those who can do so extract all the value from their resources. Those who cannot have no alternative but to trade on IRC channels where cheating is a way of life. This suggests a two tier underground economy: gangs and alliances that can extract value from their resources form the upper tier. Those who must buy resources, or who cannot monetize the credentials they steal, form the lower tier. They have no choice but to pay the tax that the rippers extract.

We find that the published estimates of the dollar value of underground economy IRC channels are exaggerated. They are derived by simply adding the unverified claims of anonymous channel participants (who include rippers). Those who lie most and exaggerate most affect the average most. We emphasize that the activities of the upper tier are largely invisible and probably account for a majority of the losses.

An important conclusion is that goods offered for sale on the IRC channels are hard to monetize. Those who sell there are clearly unable to monetize the goods themselves or find someone who will do so for a smaller premium than the ripper tax. Since stolen CCNs and bank credentials are a majority of the goods offered for sale this implies that getting credentials is only a first step, and by no means the most important one, in the chain of fraud.

We find that different means are necessary to fight the two tiers. The alliances and gangs of the upper

tier act as businesses and will respond to economic and law enforcement pressures. Those in the lower tier are harder to reach with these means. While they make little, they generate very significant externalities.

Ironically, defenders (*i.e.*, whitehats, security vendors and members of the security community) actively and energetically recruit their own opponents. By repeating unverified claims of cybercrime riches, and promoting the idea that easy money is there for the taking, we attract new entrants into the lower tier of the underground economy. While they may produce little profit they still generate large quantities of spam and phishing and cause significant indirect costs. There is a further irony that internet users, financial institutions, the security community and both upper and lower tier cybercriminals all have interests that are aligned on the matter of having accurate data free of exaggeration. This is so since an accurate accounting of their prospects might cause many in the lower tier to leave the underground economy. Most obviously internet users, banks and financial institutions would be better off and the security community could concentrate on the smaller, if abler, upper tier. Less obviously, those in the upper tier would benefit from decreased competition. Finally, those in the lower tier would benefit as they would be spared wasting their time on what, for most of them, will be a profitless endeavor. The only people who benefit from exaggerated and inaccurate underground economy estimates appear to be the rippers.

6. REFERENCES

[1] http://iang.org/papers/market_for_silver_bullets.html.

[2] http://www.cer.org.uk/pdf/wp721_org_crime_brady.pdf.

[3] Symantec Internet Security Threat Report XIII. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf.

[4] Symantec Report on the Underground Economy XII. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

[5] A. Acquisti and J. Grossklags. Uncertainty, ambiguity and privacy. *WEIS*, 2005.

[6] A. Ozment and S. Schecter. Milk or wine: does software security improve with age? *Usenix Security*, 2006.

[7] Adam Smith. An Inquiry into the Nature and Causes of the Wealth of Nations. 1776.

[8] C. Abad. The Economy of Phishing:A Survey of the Operations of the Phishing Market. *Cloudmark-TR*, 2006. http://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf.

[9] D. Geer and D. Conway. What We got for Christmas. *IEEE Security & Privacy Mag.*, 2008.

[10] D. Geer and D. Conway. The Øwned Price Index. *IEEE Security & Privacy Mag.*, 2009.

[11] Federal Trade Commission. Identity Theft Survey Report. 2007. www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[12] Ford R., and Gordon S. Cent, Five Cent, Ten Cent, Dollar: Hitting Spyware where it Really Hurt$. *NSPW*, 2006.

[13] G.A. Akerlof. The Market for Lemons: Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*, 1970.

[14] H. S. Gordon. The Economic Theory of a Common-Property resource: The Fishery. *Journal of Political Economy*, 1954.

[15] G. Hardin. The Tragedy of the Commons. *Science*, 1968.

[16] C. Herley and D. Florêncio. A Profitless Endeavor: Phishing as Tragedy of the Commons. *NSPW 2008, Lake Tahoe, CA.*

[17] J. Franklin and V. Paxson and A. Perrig and S. Savage. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. *Proc. CCS*, 2007.

[18] J. Zhuge, T. Holz, C. Song, J. Guo, X. Han and W. Zou. Studying Malicious Websites and the Underground Economy on the Chinese Web. *Proc. WEIS*, 2008.

[19] J.P. John, A. Moshchuk, S.D. Gribble and A. Krishnamurthy. Studying Spamming Botnets using Botlab. *NSDI*, 2009.

[20] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pages 3–14, Alexandria, Virginia, USA, October 2008.

[21] M. Cova, C. Kruegel and G. Vigna. There is No Free Phish: An Analysis of "Free" and Live Phishihg Kits. *WOOT*, 2008.

[22] N. Dhanjani and B. Rios. Bad Sushi: Beating Phishers at their Own Game. *Blackhat*, 2008.

[23] N. Fultz and J. Grossklags. Blue versus Red: Toward a Model of Distributed Security Attacks. *Financial Crypto*, 2009.

[24] Pierre Berton. Klondike: The Last Great Gold Rush, 1896-1899. 2001.

[25] R. Anderson. Why Information Security is Hard. In *Proc. ACSAC*, 2001.

[26] R. Anderson and T. Moore. The Economics of

Information Security. *Science Magazine*, 2006.

[27] R. Thomas and J. Martin. The Underground Economy: Priceless. *Usenix ;login:*, 2006.

[28] R.H. Coase. The Nature of the Firm. *Economica*, 1937.

[29] S.D. Levitt and S.A. Venkatesh. An Economic Analysis of a Drug-Selling Gang's Finances. *Quarterly Journal of Economics*, 2000.

[30] T. Moore and R. Clayton. Examining the Impact of Website Take-down on Phishing. *Proc. APWG eCrime Summit*, 2007.

[31] Thorsten Holz, Markus Engelberth and Felix Freiling. Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones. *Reihe Informatik. TR-2008-006*, 2008. `http://honeyblog.org/junkyard/reports/impersonation-attacks-TR.pdf`.

[32] Zhen Li, Qi Liao and Aaron Striegel. Botnet Economics: Uncertainty Matters. *Proc. WEIS*, 2008.