8

Discrediting Vendors in Online Criminal Markets

David Décary-Hétu[1] and Dominique Laferrière[2]

OVER THE PAST FEW YEARS, RESEARCHERS HAVE DESCRIBED THE CONSTANT growth of a complex virtual criminal underworld in which personal and financial data is bought and sold (Holt and Lampke 2010; Franklin et al. 2007; Thomas and Martin 2006). Hundreds if not thousands of vendors compete at any point in time to sell Visa, MasterCard and American Express numbers, very often at a low rate. Yet, the economic impact of these markets can be measured in billions of dollars (Anderson et al. 2013).

This chapter discusses how law enforcement agencies have targeted and investigated this criminal underground. While a traditional investigate-then-arrest methodology has been the method of choice of these agencies, researchers (Mell 2012; Motoyama et al. 2011) have argued that law enforcement agencies should move to a disruption model in order to increase their efficiency and increase the impact of the operations. This study seeks to understand the formation of trust of ties and business ties to enhance our ability to launch disruption attack on the criminal underground. We find that even small disruption operations may have an important impact on the activity of the offenders involved in the theft and resale of stolen financial information.

Carding and the underground economy

Carding is defined as the unauthorized use of credit and debit card data for fraudulent purposes (Peretti 2008). Known in the criminal underground as *carders,* individuals involved in such an activity usually specialize in one of two areas: the theft of financial data or the monetization of stolen information (Motoyama et al. 2011; Mell 2012).

[1] David Décary-Hétu is a Senior Scientist at the School of Criminal Sciences of the University of Lausanne. His main research interests are cybercrime, online illicit markets and criminal reputation.

[2] Dominique Laferrière is a Ph.D. candidate at the School of Criminology of the University of Montreal. Her research interests include life-course criminology and criminal trajectories.

Data thieves use a wide array of offline and online attacks to gather financial information. In the offline category, past research (Peretti 2008) has identified methods such as dumpster diving, pickpocketing, purse snatching and burglary as sources of credit and debit card data. More computer literate carders also use hacking to get their hands on financial data (Provos et al. 2007). Government and businesses frequently report that offenders have managed to access and download online databases that contained the names, addresses and credit card information of their citizens or customers. Carders can also target individuals by installing monitoring software on their computers or cell phones.

Offenders possessing the required skills to acquire illicit financial data do not always know how to transform this information into money (Dupont 2012). Hence, some carders specialize in the monetization of stolen information (Sullivan 2010). One commonly used technique is to order goods or services through online merchant websites. Authentication on these sites is often minimal, requiring only the cardholder's information, which is often sold along with the card data itself (Prabowo 2011). Another technique is to manufacture fake cards which can be used to make purchases in physical stores. The goods purchased can then be fenced or refunded for cash.

As profit is a primary motive, carders who steal financial information and those who monetize this data must meet and work together. To interact, these offenders use computer-mediated communications (CMC) like the Internet Relay Chat (IRC) and online web forums (Motoyama et al. 2011; Franklin et al. 2007). IRC is a free online text-based chatting infrastructure which allows individuals to exchange public and private messages and files. Online web forums are websites on which individuals can post public messages which are divided in topics called threads. Private conversations and file exchanges are also allowed.

Both IRC and online web forums are hosts to what Thomas and Martin (2006) labeled as the underground economy. This economy includes a number of criminal markets where participants can share their knowledge and find potential business partners (Motoyama et al. 2012). Individuals freely and openly advertise illicit goods and services such as credit card numbers, online banking logins, spam and hacking services (Vömel et al. 2010). Sellers post a detailed description of what they have to offer and other participants can then shop for the best product or service that fits their particular need (Holt and Lampke 2010). Private messages, emails and instant messaging software are used to negotiate deals and payments are made in online currencies such as Liberty Reserve, WebMoney and Bitcoins (Hilley 2006). Each market is a unique ecosystem with its own social hierarchy (Holt and Lampke 2010). All markets have *administrators* that are in charge of registrations and of handing out rewards and punishments. Some have a more elaborate structure with official titles such as *moderators* and *trusted vendors*. In this case, administrators vet market participants and grant specific roles and/or privileges to a selected few. *Regular members* are the foundation of markets and represent the vast majority of participants.

Yip et al. (2013) found that a high level of uncertainty is associated with the underground economy. This uncertainty is created by the inability of buyers to ascertain the quality of goods and services sold, and to verify the identity of market participants. Scammers and rippers – individuals who act opportunistically by not living up to their end of the transaction (e.g. not sending the stolen financial data or sending stolen financial data that is unusable) – abound in criminal markets. In an attempt to raise trust levels between participants in the underground economy, market administrators have offered to vet vendors by testing their goods and services. Sellers who fulfill the administrators' criteria are given a special title such as that of *trusted vendor* which ensures them higher prestige. Some online forums have also instigated reputation systems that mimic that of eBay and Amazon in which participants rate each other.

Trust online is based on reputation. Research has shown that reputation is not distributed randomly among forum participants (Décary-Hétu and Dupont 2013). Those with the highest level of involvement, the largest number of social ties and an ability to get noticed by forum administrators can expect to earn higher levels of reputation. Carders may use alternatives to official reputation systems to evaluate the trustworthiness of participants such as background checks, past criminal activity and the willingness to share incriminating evidence (Lusthaus 2012). Reputation can be seen as a form of capital that can be used to further develop social ties and engage in business transactions (Monsma et al. 2010). This virtual capital (Décary-Hétu 2013) is even more important in the case of carders as offenders have few other options to evaluate the trustworthiness of potential business partners.

The question of how to determine the size and financial impact of the cybercrime industry is still widely debated in academic research and corporate reports (Erbschloe 2010; Kshetri 2010). Using sellers' messages to evaluate the carding market size only offers a very rough estimate of the carding scene's dimensions (Holt and Lampke 2010). Holz et al. (2008) faced a similar problem as there is no certitude that a credit card number that is lost will necessarily be compromised. Still, the annual estimate of losses due to online fraud on UK issued cards reached US$574 million in 2010 according to the UK Cards Association (2012). A more recent report by Anderson et al. (2013) provides similar estimates, but adds that the loss of confidence associated with carding has caused over US$2 billion in loss.

Policing the Carding Markets

Over the past few years, law enforcement agencies (LEAs) have successfully disrupted a number of carding forums. The four most important operations targeted the ShadowCrew, CarderPlanet, CardersMarket and DarkMarket marketplaces. ShadowCrew was created by a 21-year-old student and a 43-year-old retired broker from New Jersey (Verini 2010). In a matter of months, it grew to more than 4,000 profiles[i], and members exchanged at least 1.7 million stolen credit card numbers between 2002 and 2004. Authorities estimate losses to be more than US$4.3 million. Launched in 2001 by a Ukrainian, CarderPlanet was the Eastern European counterpart of ShadowCrew and boasted more than 7,000 profiles (Acohido 2008). Many of these traders were recruited through an online video ad campaign. Both forums were shut down in the mid-2000s.

Emerging to fill this void, the ambitious administrator of CardersMarket (Poulsen 2011), sought to secure his position as the leader of the top carding market by hacking into four of his competitors' sites and by stealing their databases of their user profiles and messages. The activities of 4,500 carders were thereby instantly moved and concentrated into a single market. One competitor, DarkMarket, did survive this attack and continued on with its illicit activities (Glenny 2012). At its peak, DarkMarket had over 2,500 registered profiles – an impressive figure for an invitation-only forum.

To build their cases against these markets' participants, LEAs adopted different techniques. In the case of ShadowCrew, a member of the forum known online as *Cumbajohnny* was arrested through sheer luck by an N.Y.P.D. detective who was on the lookout for a car thief (Verini 2010). Gonzalez (*Cumbajohnny*'s real name) used his access to the ShadowCrew market to leverage a plea bargain with the prosecution. Through his account, the United States Secret Service (USSS) was able to anonymously monitor other members. In total, 28 members of ShadowCrew located in seven countries were arrested with the help of local and national LEAs from the UK, Canada, Bulgaria, Belarus, Poland, Sweden, the Netherlands, and Ukraine (Verini 2011).

In the case of CardersMarket, an arrested member turned informant in exchange for a plea bargaining (Poulsen 2011). He used his access to the market and his social ties to gather personal information related to the market's administrator, Max Butler, which then led to his arrest.

To take down DarkMarket, the F.B.I. also resorted to insiders, this time allowing one of its own agents to take over the account of a discretely arrested spammer (Glenny 2012). This agent built his online persona and eventually oversaw the web hosting of the market as well as the proxy used by members to anonymize their connection to the forum. This not only provided the F.B.I. with a complete picture of the forum, but also gave them access to the IP addresses of many members. In 2008, 60 members of the DarkMarket were arrested with the help of the UK, Germany and Turkey (Glenny 2012).

CarderPlanet was the only market not shut down directly by LEAs. The administrators decided to take down their forum following the arrest of two members who had managed to monetize millions of stolen credit cards. This decision was also motivated by successful police infiltration of three other major markets (Acohido 2008).

These few cases highlight LEAs' ability to disrupt online cardings forums. Despite the fact that the administrators were not always located in the United States, authorities still managed to arrest most of them, and to effectively stop the illicit trade of financial data on these specific and large-scale platforms. In addition, policing work has shown its ability to turn market participants into useful informants – once caught their members were turned into double agents or provided inside information on key participants. However, these cases also reveal issues that continue to hamper efforts to detect, investigate, and disrupt carding markets.

1. *There appears to be a great deal of luck involved in carding investigations.* In every case, market participants were arrested not because of their involvement in online carding forums, but rather because of mistakes they made while using stolen credit and debit cards. Only after they had been arrested could their true value as undercover agents be established. This vastly limits LEAs' ability to build an effective attack against carding forums, as they often seem to depend on random events.
2. *Only a handful of market participants are ever arrested.* Once informants are available, LEAs tend to focus the bulk of their operation on high ranking members of the forums

(based on official titles), the most visible participants on the forums. This is consistent with past research on strategic positioning by Morselli (2010) who found that the most visible participants are more prone to arrests. This specific targeting has not prevented the ceaseless emergence of new illicit online markets. Given the international nature of online carding forums, the required level of cooperation between countries, and the difficulties in identifying market participants, it would appear highly unlikely that an important proportion of members of any given forum could be ever be apprehended in a single operation.

3. *The infiltration/arrest technique incurs high costs, particularly in terms of human resources.* Monitoring the activities, roles and identities pertaining to all profiles on each forum requires access to and financial capacity to pay large pools of analysts who can make sense of all the collected data. Human costs of double agents who have to infiltrate the carding forums also need to be factored in. This intense participation level is necessary to build a credible online persona and to establish it them important members of the market. Such sacrifices are significant for double agents, and the availability of such individuals may limit the number of investigations that may actually be launched every year (Glenny, 2012).

Disrupting a Carding Forum

Investigations such as those exhibited in the previous section are typical of traditional police work in which investigators gather evidence, build cases and arrest offenders. Increasingly however, traditional police operations are being perceived as too slow, too expensive and too unreliable. According to Innes and Sheptycki (2004), intelligence-led policing is gaining in popularity as an alternative to traditional police operations and drives LEAs to disrupt criminal networks rather than arrest offenders. This can take the form of prosecution, but only for crimes unrelated to the core activities of the offenders. A good example would be to prosecute a drug dealer for tax evasion, neutralizing him and preventing further offending, at least in the short run.

Network disruption has been proposed as the best practice to prevent crime in online carding markets. Douceur’s (2002) Sybil attack is at the root of most disruption techniques that directly targets carding forums’ trust mechanism. Douceur studied how systems with built-in redundancy could be gamed by creating multiple fake identities. He devised how an attacker could create a large number of fake identities in networks and use their voting power to gain an edge over others. When the ratio of fake/real identities reaches a certain threshold, it becomes impossible for other participants to discriminate between real and phony users, as false information is so prevalent.

This disruption technique can be applied to online carding markets in two ways. The first, known as the *slander attack*, starts when an entity engages in a business transaction and consistently reports to third parties the opposite outcome of his dealings (Franklin et al. 2007; Soudijn and Zegers 2012). If a seller is honest and provides high quality goods, the entity conducting a slander attack would publicly label him as deviant, and recommend that others refrain from future deals with him. If the seller cheats or acts opportunistically, the entity would instead highly recommend him to others.

Alternatively, the confusingly labeled *Sybil attack* (not to be mistaken with Douceur's version) suggests that a much more intense involvement in the market is necessary for disruption (Franklin et al. 2007; Yip et al. 2013). To do so, a sufficient number of fake entities must be created on forums. Sybil attackers must build credible online personas for their fake entities and gain market members' trust. On online carding forums, this process can be greatly facilitated by gaining an official role such as that of trusted seller. This trusted status is important, as many buyers are rightfully reticent to deal with sellers who have not gained the trust of others. Past research suggests that the barriers for transactions are significantly lower once this status is acquired (Holt and Lampke 2010). Sybil attackers can take advantage the trusted status of their fake entities to engage in an increasing number of business transactions. In each transaction, Sybil attackers should act opportunistically and fail to deliver on their end of the deals. If enough fake entities defraud their customers, the trust mechanisms of carding forums would be greatly challenged, thereby reducing transactions fluidity.

Rooted in a strong theoretical framework, the Sybil attack is believed to be the best practice that should be adopted by LEAs to prevent online carding. To the best of our knowledge, Hoe et al. (2012) are the only ones to have assessed the effectiveness of Sybil attacks, but did so using a theoretical model. The authors came to the conclusion that police agencies could and should disrupt carding markets by launching a Sybil attack, and that they should take advantage of sales to gather evidence on buyers for their later arrests. According to their study, this would yield the highest return on investment.

The success of Sybil attacks relies heavily on the ability of LEAs to build ties of trust and business ties in a carding forum. Indeed, out of the five stages of a Sybil attack (registering fake identities; gaining a trusted status; engaging in business transactions as a seller; acting opportunistically in transactions; assessing the impact), at least three require strong and strategic ties be created. First, only a limited number of participants can hope to achieve a trusted status in any given forum. The value of the status relies on the level of test one must face to achieve it. In hierarchical forums where forum administrators hand pick trusted sellers, personal relationships are bound to play a role. Participants need to position themselves strategically to have both the support of the administrators and that of the other participants who can act as endorsers. Second, there is a limited pool of buyers on carding forums and trusted sellers must compete for their business. To maximize their impact, Sybil attackers need to gain the largest market share possible so that their disruptive behavior can affect the greatest number of buyers. Here again, social ties will be important to develop business relationships and to generate interest around a seller's products. Third, the structure of the social ties in a carding forum can be used evaluate the impact of Sybil attacks. A disruptive attack should reduce the number of ties and increase the distance between participants. The number of unconnected dyads and triads should also be on the rise following a Sybil attack. Lastly, while not always the case, some forums may require that new members be vouched for by an existing member. This stresses the need to build a reliable network of contacts in the carding scene in order to access forums and be granted the authorization to register one or multiple accounts on a carding forum – the first step of a Sybil attack.

The present study will build on past research on Sybil attacks and analyze the formation of ties of trust and business ties in the context of a carding forum. Understanding the formation ties of trust and business ties is essential to launch effective Sybil attacks and increase the crime prevention efforts of law enforcement. The potential of social network analysis to improve intelligence-led policing and prevent further victimization from carders by targeting the forums that have made them so efficient in the past years will be at the core of this research. Using a complete copy of a carding market which was active during the summer of 2009, we intend to analyze the processes that lead to the formation of ties of trust and business ties and to demonstrate that Sybil attacks may be an interesting disruption technique that should be adopted more widely by LEAs. Understanding how carding can be prevented is of the utmost importance.

In addition to its direct costs, financial fraud costs billions of dollars in prevention programs and monitoring (Anderson et al. 2013). Individuals, corporations and governments invest massive amounts of money to protect themselves against this type of fraud. This engenders important security costs, which should and need to be controlled.

Current Study

Data

The data used in the present study was gathered from the GhostMarket online forum. Although the forum was not exclusively dedicated to carding, most of its activity took place on its carding sub-forum. Between April 13 and July 16 2009, 3,280 profiles were registered on the forum. Out of these, 2,267 (69.1%) could be considered lurkers, as they did not post any public or private message. In total, 680 profiles (20.7% of total profiles; 67.1% of active users) either posted a public message in the carding sub-forum or sent a private message to someone who did. These profiles were considered as pertaining to active carding members.

The database containing all of the public and private messages, as well as all participant profiles was leaked online at some point following the arrest of the forum administrator and other members. The database was recovered using Google's search engine. We installed a copy of the PHPBB forum platform on our local computer, as it was used to host the GhostMarket forum when it was active. We then registered a new account and promoted it to the administrator level. This enabled us to browse through all of the data as if we actually were the platform administrator. Complete access to all of the public and private messages, as well as all of the member profiles was thus obtained.

Multiple databases were created around this data. The first one contained the carders' characteristics: their usernames, their level of involvement on the forum (number of days of activity, number of public messages posted, number of private messages sent), their market activities (the number of ads posted, seller status – a dichotomous variable indicating whether they had posted an ad) and whether they had achieved the trusted status. A second database was built around the ads posted on the forum. A total of 203 threads offered stolen financial information for sale. Each ad was analyzed to compile a list of the origin of the cards being offered for sale, whether the cards were being sold with the personal information of the cardholder (name, address, date of birth) and whether a price was advertised for the cards.

Four social network matrices were also created to explain the formation of trust of ties and business ties. The first network maps the *private messages* between carders and is a valued directed matrix. For each participant, the number of ties and eigenvector measures were calculated using the software package UCINET 6 (Borgatti et al. 2002). Eigenvector seeks to identify the individuals that connect with central actors (i.e. those with large numbers of direct contacts -Bonacich 1972). This measure been used in the past as a measure of the power each actor holds in a network.

Figure 1 : Sociogram of private messages between participants on GhostMarket

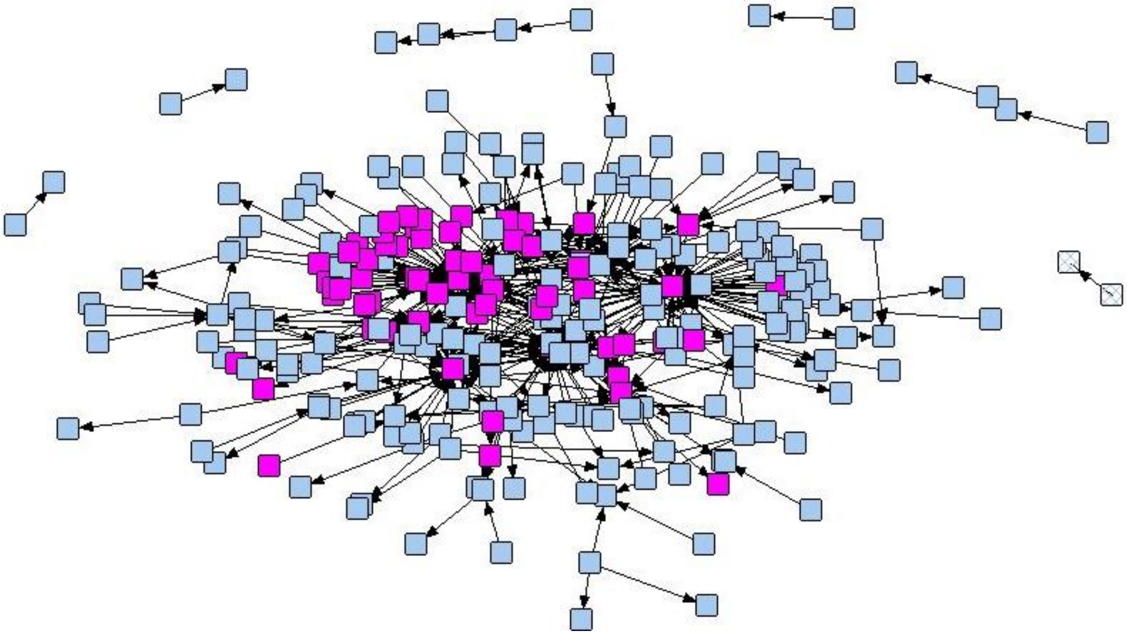

Figure 1 presents a sociogram created with the Netdraw software package (Borgatti 2002) of the ties between carders based on the private messages they exchanged. Trusted participants are in purple and untrusted participants in blue. As evidenced by the sociogram, most trusted participants are located at the core of the network and appear to play a more central role in the network.

The second network maps the *endorsements* between carders and is a directed binary matrix. To achieve the trusted status, participants were asked to publicly submit an application and wait for others to vouch for them. Officially, any participant with the support of two trusted participants would automatically achieve the trusted status but, in practice, this rule was rarely enforced. This network therefore records which participant supported which applicant. The third network maps the *business ties* and is a directed value matrix. The main role of GhostMarket was to facilitate contact between potential buyers and vendors, not to provide an exclusive transaction platform. As participants mostly relied on private email accounts and instant messaging to negotiate with one another, we were unable to monitor all the negotiations between buyers and sellers. Given this limit in the data, we opted to map the initial contacts between buyers and sellers that were initiated on both the public and private spheres of the forum. All messages – private and public – were included in order to identify which buyer had showed interest for which seller's products. These have been termed *business ties* or alternatively *negotiation ties*. The fourth and last network maps the *feedback* posted on the forum and is a directed value matrix. Holt and Lampke (2010) explain that carders leave public feedback on forums to share their experiences with vendors. Both good and bad feedback can be posted. We parsed all public messages and recorded all occurrences of feedback, both good and bad.

Assessment Method

The aim of this paper is to analyze the formation of ties of trust and business ties in the context of a carding forum. This will enable us to improve our crime prevention strategies, particularly the disruptive techniques like the Sybil attacks.

Ties of trust can be studied first and foremost through the vetting process that leads to the achievement of the trusted seller status. Indeed, carders who publicly endorse an applicant display a tie of trust between them and the applicant. In total, 103 participants applied to become trusted on GhostMarket and out of those, 57 (55.3%) succeeded.

A logistic regression was used to predict who may achieve the trusted status on GhostMarket. The predictive model includes two sets of variables: variables related to the applicant's personal characteristics and variables related to his endorsers' characteristics. The five personal characteristics included in the model are: the number of days of activity on the forum at the application date, the number of ties, the number of public messages posted, a dichotomous indicator of whether or not the applicant was known to be a seller on the forum (i.e. he had posted an ad before requesting to become trusted – the seller status) and the total number of negative feedback received publicly. The number of ties is a measure of the number of participants the applicants has interacted with through private messages. The number of ties and the number of public messages posted are used as proxies for the size of the social network of the applicant.

The second variable set refers not to the size of the social network of the applicant but to its composition. It focuses on the *type* of endorsers vouching for the applicant. Since more than one participant could endorse a particular application, it was not possible to include the characteristics of each endorser in the predictive model. In order to mitigate this issue, we sought to identify whether homogeneous groups of vouchers could be distinguished using two-step cluster analysis (Mooi and Sarstedt 2011). The cluster analysis is based on the characteristics of the endorsers and not on their own ego network. For each forum member who vouched for an applicant, we determined whether or not they were trusted, their total number of public and private messages, as well their eigenvector score based on their private messages. The analysis successfully unveiled three types of vouchers: the *administrator*, the *untrusted endorsers* and the *trusted endorsers*. Cluster quality was determined to be good. The descriptive statistics of each cluster is presented in Table 8.1.

Table 8.1 Descriptive Statistics of Vouchers Clusters

	Administrator	Untrusted Endorsers	Trusted Endorsers
Cluster size	1 (1.64%)	24 (39.34%)	36 (59.02%)
Trusted status	Yes	No	Yes
Number of public messages	1643.00	122.64	105.88
Number of private messages	860.00	74.75	97.47
Eigenvector	0.25	0.06	0.09

The first cluster encompasses only one member – the forum’s administrator. As the sole person in charge of approving or rejecting trust applications, it is reasonable to believe that his influence would be of particular importance in the process of gaining trust within this market. This is reflected by the fact that this individual makes up an entire cluster in our analysis. Investigation of associated metrics also reveals that he posted much higher numbers of both public and private messages, and that he is considerably more central in GhostMarket's network than individuals in the other two clusters. Untrusted endorsers tended to have a more visible profile by posting more public messages than the trusted endorsers (122.64 versus 105.88), but this did not translate to real power in the forum as demonstrated by the average number of private messages (74.75 versus 97.47), and by the average eigenvector (0.06 versus 0.09). Each cluster was entered as a dichotomous variable in the logistic regression model, distinguishing whether or not someone from that specific vouching group had endorsed the applicant.

The trusted status may be used to explain business ties as was suggested by Holt and Lampke (2010). Indeed, we would expect that trusted vendors would be on the receiving end of more negotiation ties than the untrusted participants. We sought to validate how the trusted status shaped negotiation ties by measuring their degree centralization. Degree centralization identifies the extent to which the recipients of negotiation ties are concentrated among a particular group – in this case within trusted and untrusted sellers (Wasserman and Faust, 1994). UCINET 6 was used to measure degree centralization (Borgatti et al. 2002).

While it is impossible to determine how many of these negotiation ties ended up as actual sales, they nevertheless allow for the identification of vendors who generated the highest level of interest among buyers. Since individuals may have trusted or untrusted status, four combinations of negotiation ties are possible: 1) untrusted buyers buying from untrusted sellers; 2) untrusted buyers buying from trusted sellers; 3) trusted buyers buying from untrusted sellers and; 4) trusted buyers buying from trusted sellers.

To further investigate the formation of business or negotiation ties, a second logistic regression was conducted in order to predict successful advertising among sellers – an indication of a higher number of business ties. This model predicts whether or not sellers were able to develop negotiation ties with buyers. On GhostMarket, a total of 136 members were defined as sellers as they had publicly advertised their products. Again, predictive factors are extracted from two specific categories: vendors' individual characteristics and the characteristics pertaining to their posted ads. The first variable set includes the total number of days active on the GhostMarket, the number of positive and negative feedback, as well as the total number of ads posted. The number of positive and negative feedback will be used as a proxy to understand the type of ties that sellers may have formed with buyers. The second variable set includes dichotomous indicators of whether vendors had included information concerning the offered credit cards' country of origin or not, whether credit card holders' name and addresses were specified or not, and whether prices of items for sale were listed or not.

The formation of business ties is likely to be affected by the events that occur in the carding forum. Of particular interest to us is the impact of the ban of a trusted seller on the formation of business ties. As the forum has been shut down by law enforcement, any empirical testing of this impact is impossible – and would raise some ethical concerns even if that was not the case. In lieu of, we used the ban records that were stored in the GhostMarket database. Administrators would, for a wide variety of reasons, ban participants who did not respect the forum's rules. Many transgressions were described as scamming behavior or serious incivility. We hypothesize that the ban of a trusted vendor will have a significant impact on the number of overall negotiation ties in the market, as well as on the number of ads posted. If Sybil attacks are to be proven as effective disruption tools, this hypothesis should be confirmed by our results. We used the Change-Point Analyzer software (Taylor 2000) which identifies time ranges in which it estimates that a change actually occurred, a confidence level surrounding this change, as well as the values of the predictive variables before and after the identified change.

Results

The formation of ties of trust can be understood through the vetting process that leads to the achievement of the trusted seller status on GhostMarket. 103 participants applied to obtain the trusted status and 57 (55.3%) succeeded. Table 8.2 presents the predictive model explaining the differential outcomes of trusted status applications. The overall model is significant (Nagelkerke R^2 = 0.476).

Table 8.2 Logistic Regression Model Predicting of Success in Obtaining the Trusted Status

	B	S.E.	Sig.	Exp(B)	STD Coefficient
Applicants' characteristics					
Number of days of activity	-0.01	0.02	0.51	0.99	-0.06
Number of public messages	0.01	0.01	0.65	1.01	0.05
Number of ties	0.02	0.02	0.24	1.02	0.13

Seller status	-0.78	0.62	0.37	0.21	-0.09
Nb of negative feedback	-1.69	0.61	0.01	0.19	-0.28
Endorsers' characteristics					
Cluster: admin	2.42	0.84	0.00	11.28	0.25
Cluster: trusted	2.07	0.70	0.00	7.90	0.24
Cluster: untrusted	2.54	0.68	0.00	12.66	0.29
(Constant)	-1.51	0.61	0.01	0.22	-0.17

N = 109

In this model, none of the applicants' personal characteristics were significantly predictive of success in gaining the trusted status, except for the number of bad references, which were negatively predictive of the dependent variable (-1.69, p = .01). This suggests that past activity and social role within the market does not increase one's chance of becoming trusted. However, displaying harmful behavior – as measured by the amount of negative feedback – did not go unnoticed among GhostMarket members, negatively impacting applications' outcomes. Endorsers' characteristics were all significantly predictive of trusted application outcome on the GhostMarket forum (Cluster admin: p = .00; Cluster trusted: p = .00; Cluster untrusted: p = .00). The standard coefficients reported in Table 8.2 suggest that being endorsed by the untrusted sellers of the forum is the best endorsement one could get in order to successfully obtain the trusted status (standardized coefficient = 0.29). The second most reliable form of endorsement to gain official trust on the forum seems to come from the administrator, and the third from the trusted participants (standard coefficient = 0.25 and standard coefficient = 0.24, respectively). These coefficients must be interpreted with great caution however, as the differences between all three clusters appear to be very small.

The trusted status may be used to explain business ties. Table 8.3 presents the status of recipients of negotiation ties. Trusted participants were on the receiving end of 73.4% of negotiation ties. A total of 77.8% of trusted participants preferred to negotiate with other trusted partners and 72.2% of untrusted participants adopted the same behavior. Indicating a clear bias towards vendors with the trusted status on GhostMarket, these results are in line with past research findings (Holt 2013; Yip et al. 2013).

Table 8.3 Distribution of Negotiation Ties

NEGOTIATION TIES	N	%
UNTRUSTED → UNTRUSTED	207	22.12%
UNTRUSTED → TRUSTED	540	57.69%
TRUSTED → UNTRUSTED	42	4.49%
TRUSTED → TRUSTED	147	15.71%

Table 8.4 extends these findings by presenting centralization coefficients for both statuses. Untrusted participants contacted others more often than they were contacted (0.44 versus 0.25), while the opposite trend is true for trusted participants (0.07 versus 0.61). Trusted participants were contacted much more often than untrusted participants as evidenced by the normalized indegree coefficient (0.61 versus 0.25). Trusted participants concentrated almost three times as many negotiations ties as untrusted participants did.

Table 8.4 Centralization by Status for Negotiation Ties

	Normalized OutDegree	Normalized InDegree
UNTRUSTED	0.44	0.25
TRUSTED	0.07	0.61

Participants who successfully achieved the trusted status nevertheless had to post ads in order to attract buyers' attention towards their products. With hundreds of ads, buyers had a wide selection from which to choose. Table 8.5 presents results from the logistic regression predicting whether or not sellers managed to establish negotiation ties with sellers.

Table 8.5 Logistic Regression Model Predicting Establishment of Negotiation Ties

	B	S.E.	Sig.	Exp(B)
Sellers' characteristics				
Number of days of activity	0.03	0.01	0.01	1.03
Received positive evaluations	1.99	0.73	0.01	7.31
Received negative evaluations	-0.90	0.46	0.05	0.41

Number of ads posted	0.80	0.39	0.04	2.22
Ads' characteristics				
Indicates cards' country of origin	0.08	0.60	0.90	1.08
Indicates details about the cards	0.12	0.59	0.80	1.13
Advertises the prices	-1.13	0.51	0.03	0.33
(Constant)	-0.51	0.68	0.45	0.60

N = 136

Table 8.5 shows that vendors' characteristics were important for an ad to succeed at generating interest from potential buyers. Three of the four variables at this level (number of days of activity: $p < .01$; receiving positive evaluations: $p < .01$; and number of ads posted: $p < .05$) were significantly and positively predictive of developing negotiation ties. Unsurprisingly, receiving negative evaluations from other members on the forum was negatively and significantly ($p < .05$) predictive of negotiation ties development. Interpretation of the impact of ads' characteristics on the development of negotiation ties suggests that who you are is of higher importance than what you actually have to offer. Two of the ads' characteristics (cards' country of origin indication, and cards' details indication) did not have a significant impact on the probability of creating negotiation ties. Indicating cards' prices significantly decreased this probability, but this could indicate that sellers who advertised prices actually charged more than what the market was willing to bear.

So far, our results suggest that the trusted status is essential in establishing one's self as a seller on the GhostMarket platform. As only a select few could achieve this status, our first regression model highlighted the importance of applicants' characteristics relative to their endorsers' characteristics. The second regression model then aimed at explaining the formation of business ties given their own characteristics and the characteristics pertaining to their ads.

The publication of ads and the formation of business ties should be affected by the events that occur in a carding. As bans are publicly announced, we should expect that the publication of ads the formation of business ties would slow down following the ban of a trusted vendors. Results found in Table 8.6 support this hypothesis.

Table 8.6 Impact of Trusted Sellers' Bans on Total Number of Ads using Change-Point Analysis

Day	Range	Confidence level	Before	After
54	(53, 57)	100%	1.2	6.2
59	(56, 59)	90%	6.2	0.3
66	(66, 67)	96%	0.3	15.0
69	(68, 69)	96%	15.0	1.0
81	(78, 92)	93%	1.0	3.53

The first column in Table 8.6 displays instances when significant changes occurred in the average number of daily ads. The second column displays a wider range of days during which the change could have occurred (the first column representing its best guess, however). As the confidence level is consistently 90% or higher, the changes detected are considered to be fairly solid. The last two columns report the number of ads posted per day before and after the change.

Overall, 5 changes were detected by the Change-Point Analyzer (Taylor 2000); three of which were increases and two of which were decreases. Coincidentally, every time the number of ads decreased, a trusted participant was banned from the forum. On the 58th day of forum's lifetime, one trusted and nine untrusted participants were banned from the forum. This is specifically one day prior to the first decline in total number of ads. On day 67, one day before the second drop in number of ads, one trusted and one untrusted participant were banned. As vendors posted an average of 1.49 ads while active on the forum, the decrease from 15.0 to 1.0 ad per day suggests that the ban of a single trusted participant can have an important and direct impact on the total number of ads posted on GhostMarket. The impact of banning untrusted participants seems to be minimal, as untrusted participants were banned almost daily without impacting the number of posted ads.

Table 8.7 Impact of Trusted Sellers' Ban on Negotiation Ties using Change-Point Analysis

Day	Range	Confidence level	Before	After
27	(26, 33)	100%	1.4	5.8
52	(49, 56)	97%	5.8	13.4
59	(57, 59)	100%	13.4	2.0
65	(65, 67)	96%	2.0	24.6
70	(68, 71)	100%	24.6	3.9
85	(80, 95)	99%	3.9	10.8

The results in Table 8.7 suggest a very similar impact of trusted sellers' bans of on the total number of negotiation ties. Here, the number of negotiation ties increased four times and decreased twice. The first drop occurred on the 59th day, one day following the ban of one trusted and nine untrusted participants. A second decrease occurred between day 68 and day 71, one to four days after one trusted and one untrusted participants were banned. Once again, decreases in negotiation ties are not unveiled when untrusted participants alone are banned. However, two significant decreases are noted when trusted participants are banned.

Discussion

The aim of this paper was to analyze the formation of ties of trust and business ties in the context of a carding forum in the hope that it would help improve our crime prevention strategies, particularly disruptive techniques like Sybil attacks. Our findings show that establishing ties of trust rests mainly on the participants' social capital. Their social networking needs to be developed strategically enough to ensure future endorsements and to avoid negative public feedback. While applicants' personal characteristics were not significantly predictive of application outcome, they still remain important. Indeed, it may appear suspicious for new and unknown participants to suddenly receive multiple endorsements from equally new and unknown participants. This is eloquently illustrated by a specific instance on GhostMarket when a trusted status applicant consistently inserted spaces before the dots at the end of each phrase. As he was unknown to most, other members scrutinized his application and realized that both his application and his endorsements had the same spaces at the end of each phrase. Participants quickly reported this irregularity, and his application was rapidly rejected as he had clearly created fake accounts to endorse his own application. Our findings also demonstrate that social networking plays an important role in the formation of business ties. Traces of personal ties can be found in the feedback that customers leave and positive relationships increased the formation of business ties while negative ones had the opposite effect. Business ties appear highly unstable as demonstrated by the impact of the ban of trusted sellers.

These results open several avenues for the prevention of carding using social network analysis:

1. Through Sybil attacks by law enforcement agencies.
2. Through a weakening of the ability of carders to process signs and signals.

3. Through the targeting of central actors in carding forums.

Sybil attacks have previously been defined as the best practice to prevent and disrupt online carding forums (Franklin et al. 2007; Motoyama et al. 2011). Our results support this claim and offer insights as to how such attacks could be launched successfully. Registering accounts on a forum and acting opportunistically whenever engaging in a business transactions are respectively steps 1 and 4 of Sybil attacks and can easily be achieved with very little resources. Gaining the trust of others, step 2 of Sybil attacks, is greatly facilitated by the reliance on endorsements by all types of carders (administrators, trusted and untrusted members). Multiple fake accounts can be easily registered and used to endorse one another. This reduces the need to interact with other members of the community and the risks of conflicts leading to negative feedback. Business ties can be increased (step 4) by using these fake accounts to leave positive feedback. Combined with a coordinated attack where profiles are maintained over time and regularly post ads, this technique would ensure that the fake profiles earn as large a market share as possible. Fake accounts could also be used to generate negative public feedback towards other trusted sellers. This would draw buyers away from other vendors and further increase the business ties of the fake accounts. This would also draw negatively the attention of market administrators towards these accounts and eventually lead to public warnings or even bans. The basic assessment of the impact of a Sybil attack we provide (simulated by the ban of trusted sellers on GhostMarket) shows the potential for prevention of such attacks. Indeed, the number of negotiation ties drastically dropped following these bans, leading us to conclude that Sybil attacks may be a powerful tool to disrupt and prevent future carding activities.

Criminal markets have long been recognized as harsh environments in which violence is omnipresent (Blumstein 1995; Werb et al. 2011). Carding markets are also believed to be inherently hostile (Yip et al. 2013; Fallman et al. 2010), and victimization is high among buyers of stolen financial information. In their case however, conflicts typically result in financial losses rather than in physical harm. Still, the tension generated by ubiquitous potential victimization in carding markets creates a high level of uncertainty among carders. This is likely to be exacerbated by the environment in which carding markets operate: the Internet. In the traditional criminal community, offenders can gauge other participants' trustworthiness by relying on distinguishing physical signs, such as the way they dress, the way they look, they way they speak, or the neighborhood they come from (Gambetta 2009). Most of these features tend to disappear in the virtual world as such signals can easily be faked. The question of identity thus arises – even though a participant may talk the talk and walk the walk, there is no telling whether that individual is a real carder, a scammer or a double agent (Yip et al. 2013). Following recently publicized cases of federal agents impersonating spammers and hosting entire markets, this inability to surely discern others' identity has even increased in the short past (Glenny 2012). In this context, virtual relationships and networking become increasingly important in online criminal markets. While it may be imprudent to trust signals emitted by a single individual, it is much more cautious to trust that signal when it originates from multiple sources who have proven their worth in the past. This helps explain why carders' characteristics have no impact on successfully gaining the trusted status on online markets, and why endorsers' characteristics do. It also opens up an opportunity for the prevention of carding activity by manipulating how signals are transmitted and processed. It would be possible for a number of fake accounts to add noise to online discussions and to confuse carders as whom can be trusted and whom to trust. Our results with their description of the formation of ties of trust and business ties provide clues as to how to abuse one's position in the network to limit the participation level of carders.

Making sense of signals is not an easy task. Official titles and reputation systems seek to help participants to assimilate and analyze the signals they receive. Our results have shown that a part of signal processing is delegated to forum administrators who appear to be better suited to disentangle real from fake signals. Indeed, administrators communicate with a larger number of participants and have spent more time on the forum than most if not all participants. As such, through the selection of who becomes a trusted vendor in the forum, administrators can shape the structure of ties of trust as well as the business ties. This delegation process provides LEAs with a central convergence point from which they can affect entire criminal communities. Trust systems and official titles are meant to streamline decision-making and increase markets' fluidity. If participants were to analyze every seller's trustworthiness before engaging in a transaction, very few transactions would actually ever be finalized. We are thus faced with a perfect example of what Morselli et al. (2007) have described as an efficiency/security trade-off. Administrators and trusted participants embody the market's core and as such are vulnerable to arrests and monitoring by the police. While Morselli et al.'s (2007) drug traffickers were protected by an outer layer of participants such as money launderers, brokers, and logistical contributors, the

Internet provides a direct access to anyone in carding forums. This reduces the protection that core key players of criminal networks typically benefit from. In some cases, administrators may develop defensive strategies that prevent law enforcement from identifying them. Social network analysis would here once again be a useful tool to understand the ties of trust and business ties that the administrators have developed with other participants and identify potential informants who could be used to monitor administrators. This technique was used numerous times in the past in traditional investigate and arrest police operations (Glenny 2012; Poulsen 2011). As these people would be close associates of the administrators, they could also be used to add noise to the forum by posting inconsistent reviews or by making false claims about the trustworthiness of the administrators and other participants.

Disruptive attacks, empowered by our findings on the formation of ties of trust and business ties, hold a much greater potential than the traditional investigate and arrest technique that has been used in the past to shut down online criminal markets. Data from GhostMarket suggests that carders may have come from as many as 108 countries. Arresting the hundreds or thousands of participants involved would be a daunting task, even if they originated from the same country. Coordinating a strike against them in tens of countries appears to be nearly impossible. Past police operations have focused on carding forums' top administrators and this has successfully led to the destruction of numerous online markets such as CarderPlanet, ShadowCrew, DarkMarket and CardersMarket (Yip et al. 2013; Poulsen 2011; Glenny 2012). However, these operations have not stopped mid-level and low-level participants from launching new forums. LEAs are therefore engaged in an endless war in which two forums with more stringent registration policies are created for each forum that is taken down, further limiting double agents infiltration ability. Yip et al. (2013) posit that if carders keep using carding forums even after all of these police operations, it is because online forums provide them with advantages they could not get as easily and as cheaply elsewhere: a regulation body, social networking possibilities, a basic level of identity checking, as well as a basic level of goods' quality assessment. Using disruptive techniques such as the Sybil attack, investigators would target the underlying trust mechanisms allowing these forums to incessantly surface. These methods erode the trust that carders have in these systems, thus reducing their overall attractiveness. Given the ingenuity of online offenders, new networking and co-offending schemes would undoubtedly arise sooner or later. In the meantime, however, the ensured perturbation of networks would contribute to lower levels of victimization within the general population.

Conclusion

The previously presented results highlight that understanding how virtual criminal networks could be disrupted is an exciting and highly promising field of research. Future studies should take advantage of the recent alliance between computer science and criminology in order to build simulation models that would provide better estimates of the impact of disruption attacks such the Sybil attack on online markets. Agent-based models could take into account a multitude of factors and precisely evaluate how many forum members abandon their illicit implication when trusted participants are banned, and how their online activity fluctuates through time.

Further research should also focus on the extent to which carding markets are really *lemonized*. Herley and Florêncio (2007) recently debated whether victimization among carders was so high that outside help was not actually needed to destroy online illicit forums. In other words, online markets would simply self-destruct over time, as too many scammers are involved. Our study helps understanding how police agencies (and scammers) could game the system in order to gain an advantage. The natural disruptiveness of these markets needs to be taken into account in future evaluations of Sybil attacks in order to precisely identify the level of energy required to disrupt carding and stop the flow of victimization.

The data used in this study were limited by the lack of information concerning the actual number of transactions that unfolded between sellers and buyers. GhostMarket's role was clearly to facilitate the meeting of financial data thieves and monetizers. While there should logically be a very high correlation between the number of negotiation ties and the number of transactions that took place through GhostMarket, readers should remember that exact information about the number of transactions and illicit revenues were not available to the researchers. Moreover, data were collected after the forum was officially shut down. While we have no reason to doubt the validity of the data, it is possible that the recovered database was modified to hide the nature of certain participants' roles. However, given that all public and private messages relating to carding were analyzed by the researchers, it would have been very difficult for a third-party to tamper the data to obfuscate the presence of an important player.

Trust systems appear to be online carding forums’ Achilles heel, and will thus represent an interesting research question in the years to come. While carders are sooner or later bound to realize the potential liabilities of these systems, they will still need them in order to reduce their victimization probabilities. Trust systems are carders’ catch-22: the very same systems that protect them from peers actually expose them to LEAs. Over the next few years, it will be interesting to study the innovations carders come up with to reduce their detection chances, all the while protecting themselves against scammers’ and rippers’ opportunistic behavior within their own virtual community.

References

Acohido, B. (2008). *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity*. New York, USA: Sterling Publishing Co.

Akerlof, G. A. (1970). "The Market For "Lemons": Quality Uncertainty And The Market Mechanism*." The Quarterly Journal Of Economics*. 488-500.

Anderson, R. & C. Barton & R. Böhme & R. Clayton & M. J. G. van Eeten & M. Levi & T. Moore & S. Savage. (2013). "Measuring The Cost Of Cybercrime." *Proceedings of the 11th Workshop On The Economics of Information Security.*

Blumstein, A. (1995). "Youth Violence, Guns, And The Illicit-Drug Industry." *The Journal of Criminal Law and Criminology*. 86(1): 10-36.

Bonacich, P. (1972). "Factoring And Weighting Approaches To Status Scores And Clique Identification." *Journal Of Mathematical Sociology*. 2(1): 113-120.

Borgatti, S.P. & M. G. Everett & L. C. Freeman. (2002). "Ucinet For Windows: Software For Social Network Analysis." Harvard, MA: Analytic Technologies.

Douceur, J. R. (2002). "The Sybil Attack." *Peer-to-peer Systems*. 2429: 251-260.

Dupont, B. (2012). "Skills And Trust: A Tour Inside The Hard Drives Of Computer Hackers." Available at SSRN 2154952.

Erbschloe, M. (2010). "Economic Consequences." IN Ghosh, S. & E. Turrini. (ed). *Cybercrimes: A Multidisciplinary Analysis*. Berlin, GER: Springer.

Franklin, J. & A. Perrig & V. Paxson & S. Savage. (2007). An Inquiry Into The Nature And Causes Of The Wealth Of Internet Miscreants. *ACM Conference On Computer And Communications Security*. 375-388.

Gambetta, D. (2009). *Codes Of The Underworld: How Criminals Communicate*. New Jersey, USA: Princeton Press University.

Glenny, M. (2012). *Darkmarket : How Hackers Became The New Mafia.* New York, USA : Random House.

Florencio, D. & C. Herley. (2007). "Nobody Sells Gold For The Price of Silver: Dishonesty, Uncertainty and the Underground Economy." *WEIS.*

Hilley, S. (2006). "The Shadowcrew: Organized, Yes, But 'Organized Crime'?" *Infosecurity Today*. 3(1): 10.

Hoe, S. C. & M. Kantarcioglu & A. Bensoussan. (2012). "A Game Theoretical Analysis Of Lemonizing Cybercriminal Black Markets." *Decision And Game Theory For Security*: 60-77.

Holt, T. J. & E. Lampke. (2010). "Exploring Stolen Data Markets Online: Products And Market Forces." *Criminal Justice Studies*. 23(1): 33-50.

Holz, T. & M. Engelberth & F. Freiling. (2008). “Learning More About The Underground Economy: A Case-Study Of Keyloggers And Dropzones.” *Lecture Notes In Computer Science*. 5789: p.1-18.

Innnes, M. & J. W. Sheptycki. (2004). “From Detection To Disruption: Intelligence And The Changing Logic Of Police Crime Control In The United Kingdom.” *International Criminal Justice Review*. 14:1.

Joshi, M. (2006). *Black Cards Forensics*. Navi Peth, India: Indiaforensic Research Foundation.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional And Strategic Perspective*. Berlin, GER: Springer.

Meijerink, T. J. (2013). “Carding: Crime Prevention Analysis.” Downloaded on May 1st 2013 on: http://essay.utwente.nl/63027/1/Understanding_processes_of_carding_versie_7_31-1_word.pdf.

Mell, A. (2012). “Reputation in the Market for Stolen Data”. Discussion Series Paper, Department of Economics, University of Oxford.

Mooi, E. A. & M. Sarstedt. (2011). *A Concise Guide To Market Research: The Process, Data, And Methods Using IBM SPSS Statistics*.” Berlin, GER: Springer-Verlag.

Morselli, C. (2007). “Inside Criminal Networks.” New York, USA: Springer.

Motoyama, M. & D. McCoy & K. Levchenko & S. Savage & G. M. Voelker. (2011). “An Analysis Of Underground Forums.” *Proceedings Of The 2011 ACM SIGCOMM Conference On Internet Measurement Conference*.

Peretti, K.K. (2008). “Data Breaches: What The Underground World Of “Carding” Reveals.” *Santa Clara Computer & High Tech Law Journal*. 25(2): 375-413.

Poulsen, K. (2011). *Kingpin: How One Hacker Took Over The One-Billion-Dollar Cybercrime Underground*. NY, USA: Crown Publishing.

Prabowo, H. Y. (2011). “Building Our Defence Against Credit Credit Card Fraud: A Strategic View.” *Journal Of Money Laundering Control*. 14(4): 371-386.

Provos, N. & D. McNamee & P. Mavrimmatis & K. Wang & N. Modadugu. (2007). “The Ghost In The Browser: Analysis Of Web-Based Malware.” *Proceedings Of The First Conference On Hot Topics In Understanding Botnets.*

Soudijn, M. R. & B. C. T. Zegers. (2012). “Cybercrime And Virtual Offender Convergence Settings.” *Trends in Organized Crime*. 15(2-3): 111-129.

Sullivan, R. J. (2010). “The Changing Nature Of U.S. Card Payment Fraud: Issues For Industry And Public Policy.” Downloaded on July 4th 2012 on: http://weis2010.econinfosec.org/papers/panel/weis2010_sullivan.pdf.

Taylor, W. (2000). “Change-Point Analyzer 2.0 shareware program, Taylor Enterprises, Libertyville, Illinois.” Downloaded on July 4th, 2012 on: http://www.variation.com/cpa.

Thomas, R. & J. Martin. (2006). “The Underground Economy: Priceless.” *USENIX: Login*. 31(6): 7-16.

Tremblay, P. (2010). *Le délinquant idéal.* Montreal, Canada : Liber.

UK Cards Association. (2012). “Annual Report 2012.” Downloaded on July 4th 2012 on: http://www.buzzwordcreative.co.uk/UK-Cards-Annual-Report-2012/html/index.html.

Verini, J. (2010). “The Great Cyberheist.” Downloaded on July 18th 2013 on: http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=1&.

Verizon. (2011). "2011 Data Breach Investigations Report." Downloaded on September 27th 2012 on: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

Vömel, S. & T. Holz & F. Freiling. (2010). “I'd Like To Pay With Your Visa Card: An Illustration Of Illicit Online Trading Activity In The Underground Economy.” *Universität Mannheim/Institut für Informatik.*

Wall, D. S. (2007). *Cybercrime. The Transformation Of Crime In The Information Age*. Cambridge, UK: Polity Press.

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods And Applications (Structural Analysis In The Social Sciences)*. Cambridge, England: Cambridge University Press.

Werb, D. & G. Rowell & G. Guyatt & T. Kerr & J. Montaner & E. Wood. (2011). “Effect Of Drug Law Enforcement On Drug Market Violence: A Systematic Review.” *International Journal of Drug Policy*. 22(2): 87-94.

Yip, M. & C. Webber & N. Shadbolt. (2013). “Trust Among Cybercriminals? Carding Forums, Uncertainty And Implications For Policing.” *Policing and Society*. Ahead-of-print: 1-24.

[i] It is impossible to know how many accounts were duplicates or registered by law enforcement agencies and security experts. The number of actual carders is therefore likely to be lower than 4,000.