COMS30038 — SECURITY BEHAVIOURS

SECURITY ECONOMICS: CYBERCRIMINAL ECONOMIES

Matthew Edwards[*]

---

1 A STUDY IN SPAM

In the first part of this lecture we are going to talk about how cheap Viagra pills led to the creation of sprawling cybercriminal empires involving competitive malware strains fighting for millions of compromised machines and producing multiple millions of dollars in annual revenue. That is, we are going to talk about spam, and in particular the economy that made spam possible – the different contributors and components involved in spam delivery.

Spam is at root a form of advertising. The basic premise of advertising is that if you tell a lot of people about your product some of them will be more likely to buy it. Exactly what makes advertising work is a whole field of study in itself[1], but certainly one part of the equation is a balance between the expected cost of a campaign and the expected returns in terms of *conversion* – new customers following up on the advert and buying your product. Advertisers try to balance their approach. A more expensive campaign—better researched, better produced—might convert a greater proportion of the people who see it, for example. Convincing people your product is more valuable might allow you to sell it for more money[2]. Spam takes an entirely different approach. Rather than producing a well-targeted, highly-attractive advert for an expensive high-quality product, spam aims for individually very cheap advertisements for what are usually very cheaply manufactured products. As each spam 'advert' is so cheap, it doesn't matter if the vast majority of them are filtered or ignored – the tiny percentage of conversions can easily be enough to recoup the spammers' losses. We can be pretty confident this works – estimates of the value recouped by spammers worldwide have hit as high as $200 million [2].

So, spam is essentially a breed of advertising gone wild, and in some ways quite a lucrative strategy. Given we already have some cheap product to sell,

[*]matthew.john.edwards@bristol.ac.uk

[1]And one which has a lot of overlap with the social engineering lectures.

[2]Perversely, just setting a high price for a product also gives people the impression that it must be higher-quality [1].

like a generic pharmaceutical, knockoff Rolex or piece of cracked software, what else do we need? To carry out a spam campaign requires four different elements: a list of addresses to send the email to, an email advertising your product, some sort of delivery mechanism for sending the emails, and an online shopfront you can sell your product through when someone clicks on on the link. Each of these elements forms the basis of some specialised work that has to be carried out, and therefore has a role in the economy. Sometimes these roles are clearly delineated, with different groups producing each component, and at other times large players attempt to capture more of the market themselves by handling multiple components, but either way the work has to be done and rewarded financially.

First, the email addresses. To send millions of emails and at least have a chance of them reaching potential customers, you need to have a list of millions of unique email addresses. Email addresses are therefore goods with value in the spam world, and accordingly there is an industry and a market for lists of email addresses. Workers known as 'harvesters' specialise in crawling various sources—predominantly the web—for email addresses that can be targeted by spam campaigns. Of course, not all email address lists are equally valuable, and the price of bundles of a million addresses can range from $25 to $50 [3]. Factors affecting price include validation of addresses (i.e., they are not old or automatically-generated, but route to real people), whether they have been recently targeted by other spam campaigns (less likely to make good targets), their geographical location (shipping restrictions for physical goods), and the type of email account (webmail providers like Gmail have much better spam filtering, and so addresses on those domains are less valuable) [3]. Interestingly, harvesters differ a lot in the efficiency of their delivery of harvested email addresses to market, with some of them having a turnaround time of only a few days before addresses are used in campaigns, and others holding on to addresses for more than a year – possibly because new harvesters struggle to establish the reputation necessary to attract spammer clients [4].

If we don't want to be beholden to a harvester, we could always try to do the work ourselves. Some of the first "spamware" was software for gathering email addresses, starting with 'Floodgate' in 1995, which at the time sold for $100 [5]. There are even open-source harvester programs like 'ECrawl'. However, manually gathering data takes time, and a campaign using a list gathered using default tools is unlikely to have a good conversion rate[3] – good harvesters focus on finding previously-untapped sources of email data they can crawl. To get around anti-crawling measures, harvesters often use distributed crawling architectures spread over multiple machines (owned or compromised), and have been seen spoofing the Google bot[4] and even operating from inside a Google AS [4]. As a spammer, finding a good harvester can be hard, and spammers tend to stick with a single harvester for a long

[3] Good for spam, that is.

[4] Commonly whitelisted for search indexing purposes.

time, suggesting a form of customer loyalty exists in the market [4].

Next, the spam email. It was once the case that identical messages could be delivered everywhere, but content-based anti-spam techniques find this very simple to counter – once thousands of identical messages start arriving in inboxes and being flagged as spam, mail delivery agents can quickly be informed that this message is undesirable and start refusing to deliver it. A naive approach to writing your email is also likely to sound a lot like previous spam emails, and be caught by existing spam filters. As such, any halfway sophisticated spammer is going to want to provide a spam *template* that sets out the general form of the message they want to deliver, but with areas of content that can be mutated as required during the campaign to get around filtering technologies [6]. The market works hard to make such templating accessible. For example, the Curtwail botnet provided a web interface to assist customers in creating their spam template, allowing them to specify different headers and content using macros. The template created by the user was then passed through a local copy of *SpamAssassin*[5], to judge whether it was likely to make it through to inboxes, and could be interactively tweaked until this was possible [3]. These services are often offered by the spam distributors to their customers, and can be a point of competition – an easy-to-use interface and good technical support[6] can differentiate your service from others on the market, and help attract and lock-in customers.

This brings us to the big one: spam delivery. Technically, just about any internet-connected machine could set up a mailserver and start sending bulk unsolicited email as fast as the network allows. Practically, however, such a machine would be quickly *blacklisted* by anti-spam measures, and no longer be of any use to the spammer. This is one of the most effective measures for preventing spam, and cuts out masses of email – about 80% of all email received by Yahoo! Mail in 2011 was deflected by IP blacklists [5]. Spam delivery specialists therefore have had to innovate. One approach is to create accounts on reputable webmail providers, and use their reputation and infrastructure – but this can be readily combatted with CAPTCHAs that prevent automated signup, and quick clamp-downs on misbehaving accounts. Another approach is the whack-a-mole strategy, in which you use one machine to send spam until it is blacklisted, and then pop up another one – but this causes you to constantly burn IP addresses, which isn't very sustainable. A far cheaper and more reliable solution is to use a botnet.

A botnet consists of thousands of devices, usually (but not always) personal computers, which have been compromised in some fashion and—without their owner's knowledge—take part in criminal activity at the direction of the botnet master. Spam botnets in particular began appearing from around 2003 [5], and formed much of the core of the economy we're discussing. As these machines are usually on dynamic IP addresses, they cannot be blacklisted in the

[5] A spam filter, here being misused to fine-tune spam.

[6] Yes, they have instruction manuals and dedicated support teams to help their customers have the best spamming experience.

same manner as static addresses[7], and so they make for an excellent delivery system – a spam engine sits idle on a compromised host until it receives communications from a control server, which passes on a list of email addresses and a spam template. The spam engine then starts sending email. Periodically, it will check its own reputation on public spam blacklists, and report this back to the control server to give a real-time impression of its own value in the botnet [3]. The question being weighed in this case is whether it is worth continuing to give this bot spam to send, or whether it should shut down and idle again.

The value of a spam botnet depends on its capacity to deliver spam, which in turn therefore depends on the number of accessible bots within its network. As compromised machines can routinely be turned off, disconnected or cleaned of malware, the natural tendency of a botnet is to decay – sometimes by up to 50% a day. Capacity must therefore be maintained through growth, with new *loads* of the spam botnet engine being regularly delivered to fresh machines. Accomplishing this is a task requiring some specialised skills, and therefore while some botnet operators do develop their own techniques, many outsource this work to other providers, paying for *installs* [7]. This is typically accomplished by affiliates who work to drive web traffic to pages with drive-by-downloads of specialised *loader* malware, that can then be used to install other malware, but other methods of installation are equally valid and a point of competition. There is even evidence of a degree of arbitrage in the install market, as *pay-per-install* providers sometimes buy installs from each other to fulfill jobs, and some traders have been seen buying installs from a provider only to sell them back to them at a later date [7]. The market supports surprising degrees of brokerage, with some chains involving affiliates who carry out an install selling to pay-per-install services, who resell them to botnet operators, who then in turn rent out the use of their botnet to spammers, who may themselves be a service provider offering advertising to multiple online shops – many of whom might be buying their products from a manufacturer.

Competition between spam botnets for market share can be fierce and underhanded. Strains of malware have been seen which, once installed, attempt to patch vulnerabilities used by other malware families, to avoid 'losing' the machine to a rival. Of even more concern, for cybercriminals, is the risk of their control of a botnet being subverted by another gang compromising their servers, or even just bribing some of their employees to turn coat and take some substantial piece of infrastructure with them. Infighting among botnet operators was a significant limiter on their productivity during the heyday of spam, and was only made more fierce by the fact that the number of middlemen in the spam chain put a strict cap on the number of people who could get very rich – this was not an easygoing positive-sum market, this was a fierce competition for spam money[8].

[7] There are dynamic IP blacklisting approaches, but they can't completely prevent botnet traffic due to the large numbers of hosts and the nature of dynamic IPs.

[8] For more on the history of this conflict, see [8].

An important part of the spam value chain is the link that the potential customer clicks on in the email. While in some cases this leads directly to the online shop, this often makes it too easy for the domain or host to be simply taken down, so spammers make use of redirection services to obfuscate the target and help keep traffic arriving at their shop despite takedowns. These redirects are often found within legitimate third-party free hosting domains, which enable spammers to quickly set up page redirects at no (or little) cost, but can't be completely shut down because they also host a lot of normal web content. Special 'fast-flux' registrars are also used for domain names, in cause the sellers need to quickly move machines [9]. In these cases, and to some degree also with hosting, 'legitimate' third-party businesses are part of the spam economy, being paid for services that ultimately are used indirectly for supporting crime.

Next, the online retailers themselves. To run an online business for something like cheap pharmaceuticals you need four key things – a supplier, a website, a payment processor and a delivery system. Web hosting was discussed above, and a supplier can usually be assumed. The two interesting elements for security researchers are the payment processors and the shipping companies involved in this part of the spam economy, as they both control the flow of money into the system. Of course, with any business, you also need to take care of your customers and handle issues like refunds, their deliveries not arriving, et cetera. The online pharmacies not only did this (yes, with dedicated customer support numbers) but apparently did it rather well. The online businesses that advertise through spam make the majority of their money through *repeat business* from satisfied customers, and so customer experience is a significant priority for them – they are very willing to give refunds, reship failed deliveries and otherwise do whatever they can to win a customer's loyalty – as documented extensively by Krebs [8], they are in many ways more pleasant to interact with than properly-licensed pharmacies.

Now to the crux. By painstakingly analysing this spam economy, researchers discovered a bottleneck. Looking at the distinct service providers involved in the online retail that funded spam, they examined the percentage of the market that relied on particular service providers. For example, about 30% of sites used one domain registrar – relatively concentrated, but then registrars are quite plentiful and easy to set up, so shutting the registrar down might not have that big of an impact. When they looked at payments, however, the picture was more extreme. 60% of all online shops used just one payment processor to gather their funds. The top three banks in the system accounted for *over 95%* of the business [9]. There are lots of banks, but very few that are willing to process "high risk" transactions like the ones generated by these spam-advertised businesses. Banks are not easy to set up, and are subject to a lot of scrutiny by different authorities. By leaning on Mastercard and Visa to essentially blacklist the few payment processors willing to work with the

spammers, the entire spam economy could be throttled[9].

This is a golden example of the economic analysis of cybercrime paying off – by carefully examining how money flows into the system, it becomes possible to implement a relatively small intervention that throws it into freefall. However, there's also another lesson. Consider this: why were online pharmacies (in many ways the lifeblood of the spam business, though they were by no means the only thing advertised this way) so viable as a model? The Indian pill factories they fronted for were in no way market-beaters, they churned out generic drugs with low quality-control. The majority of customers were Americans [10], and the majority of drugs they were ordering from these online pharmacies were simple prescription drugs stocked by any US pharmacy. Looking at the types of drugs ordered, three different explanations arise. First, there are drugs like painkillers, which can be abused recreationally, and can be difficult to get an ongoing prescription for. Addiction or recreation may play a role in explaining this category, but this is a relatively small proportion of purchases. Next, there are drugs like Viagra which, while available, might be embarrassing to discuss with your doctor. These make up the majority of orders. Tracing the causal chain, it is entirely possible that if people were less embarrassed about erectile dysfunction, their computers would not be being regularly compromised by Russian cybercriminals. Finally, and more soberly, a smaller but still significant proportion of sales are of treatments for chronic health conditions [10]. These customers are not addicts or party-goers, and they are not embarrassed about their condition. There are very few people who would trust their lives to a shop they found via a dodgy email, if they had any other option. The only real explanation for this behaviour is that these people simply cannot afford these necessary prescription drugs under the US healthcare system.

2 TRUST & TRADE

In the above, I sometimes mentioned cybercriminal markets, but I did not expand much on what this means. In economics, a market is simply a mechanism that enables trade between different parties, and can take many forms. In some markets, goods and services can be exchanged directly through barter, while in others we see a form of currency used to allow customers to buy from vendors. Cybercriminals have both kinds of markets, and some particularly interesting forms of currency. As market economics has a big impact on the ability of cybercrime to organise and produce large, sophisticated acts of cybercrime, it can be particularly instructive to observe these markets. To explore how they work, we'll look at a selection of related cybercriminal marketplaces.

[9] Unlike fraud victims, spam business customers are unwilling to pay for spam-advertised goods through bizarre methods like gift cards or cryptocurrencies – they want to pay with methods they understand, like a credit card.

Month	*Amex*	*Visa*	*MasterCard*	*Discover*
2005/10	70	28942	11820	1064
2005/11	51	31932	13218	1214
2005/12	89	26492	10662	1079

Table 1: Breakdown of observed trade by card type [11]

2.1 *IRC Carding Markets*

One of the first major analyses of a cybercriminal market was a 2006 analysis by Thomas & Martin [11] which observed the trade in stolen credit card details taking place on IRC networks. One of their major observations was just how much of this trade there was – in just three months of observing just one IRC server, the researchers observed over 120,000 compromised card details traded, as broken down in Table 1. IRC servers like the one observed form networks with other servers, each with their own trade, and there were at the time estimated to be 35-40 easily-accessible *networks* dedicated to trade in compromised cards.

Markets are where the prices of goods are established. The value of credit card or other financial account information in this market varies based on how complete the information is on the account holder. Some card information is only useful if you want to clone the credit card physically, a fairly laborious task. Just having the username and password for an online account won't allow you to get around any additional checks a bank might make once they notice suspicious activity – for that you need more complete information, like the answers to the secret questions arranged with the bank. Vendors also, like in other markets, offer incentives for their product, with bulk discounts for large purchases – it's more efficient and safer for them to move their product in large transfers.

Markets like this one, where individuals communicate as well as trade, are also a means of learning new information for free. Traders learn about services from each other that are supportive of cybercrime, like offshore banks where they might be able to protect their money from governments and law enforcement. They also learn about which traders in the market they can trust. Trust is fundamental to trade – you need to trust that someone will pay you before you give them your goods, and you need to trust that someone will give you goods before you pay them. Given the nature of cybercrime as a business formed of actors willing to break norms around property or deception, forming trust is a particularly significant problem in this sort of market. In offline markets, traders can appeal to higher authorities if a deal is welched on or fraud attempted, and the common knowledge of this and the associated punishments keeps traders (somewhat) honest. In the IRC networks, the trust mechanisms were typically a self-regulating process, with 'rippers'[10] condemned publicly by defrauded or even just concerned traders,

[10] As in "rips you off".

and the hope being that future unwillingness to do trade with a ripper will hurt them. Of course, one of the problems with this is IRC, like most online services, is a pseudonymous medium, and it is comparatively trivial for a ripper to arrive from a new IP address with a new identity, shedding their bad reputation.

While a major element of the IRC markets is advertising card details for sale, there are other secondary services that enable this economy – specialisations that allow people without their own source of credit card details to make money from their sale. The two major specialisations in the carding market are the *cashiers* who extract funds from compromised accounts safely and the *drops* which physically reship goods ordered using stolen accounts, or otherwise launder proceeds. Other services sold in the market include verification – individuals or bots which can verify that a sample of the credit card details being advertised are genuine, giving the buyer reason to trust the seller actually has a product worth paying for.

Cashiers are necessary for extracting funds from a variety of account types, including sometimes physically going into a site like a Western Union office to claim money. As the cashier associates themselves with the crime at the point of extraction, they shoulder a lot of the risk, and so they take a large cut (typically 50%) of any account they help extract funds from. As cybercrime is dominated by males, but the victims of cybercrime generally match the population, there is a gender imbalance, and cashiers who are (or can pass as) female are therefore in demand and can charge a premium[11].

A cashier focuses on getting liquid funds out of an account. This is lucrative, but also risky, as banks will flag large cash withdrawals and similar activity. An alternative to extracting money directly is to buy goods with it, ship them to a private address, and have someone at that address reship the goods to you. You can then sell them to recoup some of the value. Drops again are associated directly with the goods bought with stolen details, and so they take a cut for this exposure and the labour involved in reshipping – between 30-50%. Location is important for drops, as there are often shipping restrictions for online purchases, or at least warning flags for merchants when an account attempts to ship goods internationally. It is also worth noting the level of trust necessary to engage in selling and buying this sort of service. Drops are physical locations, in some cases home addresses, which can be dangerous to give out online, especially if there is any chance that the person you are talking to is really a police officer.

2.2 *Carding Forums*

IRC-based markets, while still around, have slowly lost favour within the carding community, and the more common form of this market now are

[11] Though this situation is now changing – banks in the US and elsewhere are now wary of offending a customer who doesn't seem to be the gender their account would indicate, making extraction of funds from female accounts easier for cybercriminals.

online carding forums, which offer slightly better mechanisms for openly tracking user reputation. On an IRC network, communications are only recorded by clients present at the time, most channel participants are essentially ephemeral, and it is hard for a new trader to understand who is and is not trustworthy in a channel[12]. A web forum, on the other hand, has a log of public communications, and even in-built reputation-tracking systems that show you how established a user is, and whether they have a history of good trades.

The essential dynamic of sales in these forums is that a vendor with card details to sell will create a thread to advertise their goods, often attaching a sample in order to indicate authenticity. Customers then reply to initiate a transaction, either on the thread itself or, more usually, via a private message. Problems with the product, or 'vouches'[13] in favour of the vendor might be left as part of the discussion on the public thread, helping contribute to the reputation of the seller.

The goods on carding forums are relatively similar to those on carding IRC servers, as might be expected. Three main categories can be seen:

CVVs are credit card numbers, including all the information printed on the card like the cardholder name and the security code.

DUMPS are scans from the magnetic strips of cards, which can be obtained by physically skimming a card in a shop, and used to clone the card.

FULLS are complete financial account captures, including detailed personal information on the individual account holder, allowing someone to convincingly answer security questions or otherwise engage in "identity theft".

The prices for these categories tend to differ. CVVs are now some of the cheaper categories of card information, and have been getting cheaper over the years, sometimes being sold for less than a dollar, depending on other factors like the type of card, how recently it has come to market, and the region it is valid in [12]. Dumps and fulls have higher prices, reflecting the easier access to the funds in the targeted accounts.

One of the most significant properties of the carding markets is that the reliance on reputation tends to concentrate sales in a few high-profile sellers. Researchers have founds that up to 70% of sellers advertising goods on these forums attract no obvious business, and the top few sellers dominate 40-50% of all sales [12]. This is a substantial imbalance, causing some inefficiency in the market – if a new player arrives who technically would be capable of competing, and thus lowering prices, they may nonetheless struggle to attract customers simply because they are new, unknown, and thus risky to purchase from. New sellers are caught in a Catch-22: they can't sell goods because they

[12]Though there are methods of conferring status, like operators or 'voiced' users, which can be informally adopted as signals of trustworthiness.

[13]As is "I can vouch for...".

don't have reputation, and they can't get reputation because they can't sell goods.

One of the systems that be employed to help mitigate this inefficiency in the market is to use an *escrow* system. In an escrow system, a trusted third party (typically the administrator of the carding forum) is used to facilitate trade between two parties that cannot be sure of trusting each other. Funds for a purchase are handed from the buyer to the facilitator, who confirms to the seller that the funds are received. The seller then sends the goods to the buyer. When the buyer confirms that the goods are received as expected, the facilitator releases the funds to the seller, minus a small cut as a fee for their services. This tends to reduce risk for both parties in the trade, and helps enable new sellers. However, in carding markets these services currently seem to be underused.

2.3 *Cryptomarkets*

Some of the traditional problems for cybercriminal markets have included the financial system investigating stolen accounts and tracing stolen funds, creating a time-sensitive downward pressure on the value of their goods, and law enforcement finding and shutting down servers that enable trade, or using them to find vendors, creating a range of safety concerns for engaging in trade that limited the size of the market only to the more confident or risk-seeking. Around 2011-2012, the face of this issue shifted significantly. Two long-term projects within the cypherpunk movement had converged as a solution to both these issues. On the one hand, Bitcoin, a decentralised, cryptographically-backed currency, had become viable as a means of purchasing goods or services in a manner that traditional financial authorities could not interfere with – there was no bank account to freeze, and no need to trust a comparable service operator. On the other, anonymised routing had finally taken off with the (US-government-backed) TOR project, enabling the creation of "hidden services" that were addressable within the network without the client or the server ever knowing each other's IP address – creating a disconnect that resisted law enforcement efforts to locate and seize the servers that enable cybercriminal trade to take place.

These two technologies, combined, created the cryptomarkets – underground marketplaces hosted as hidden services, paying for goods with cryptocurrencies, buyers always rating sellers, making consistent use of escrow systems, and securing communications using PGP encryption. While some do carry card details and more traditional cybercriminal goods, one of the major categories of trade that emerged was the online drug trade, with the last mile of the drug distribution network being shifted to a safer environment. Increased safety – both from drug dealers and law enforcement – helped encourage purchases from the cryptomarkets. The first Silk Road had an impressive 2-year run despite a massive amount of law enforcement interest, and its many successors seem to have thrived despite several attempts at

crackdowns.

Despite the increased safety and security of the cryptomarkets, scams are still an issue for business, primarily due to weaknesses of the escrow system in use. First, the escrow system on several cryptomarkets was often slow, as the administrators were not equipped to properly handle the volume of trade. Vendors would therefore sometimes ask buyers to "finalise early" – that is, confirm to the system that funds could be released from escrow before their goods had arrived. Despite this essentially negating the purpose of the escrow system, buyers could sometimes be convinced to agree, especially if they thought they had a good relationship with the seller. One common pattern is for a vendor to make money legitimately selling goods on the market, announce a large sale on the condition of early finalisation, and then leave with the free funds gathered from the rush of business – essentially cashing out their reputation.

After the first Silk Road's high-profile takedown, the number of sellers on competitor and newcomer markets *increased*. Following attempts to close down these markets have had local successes, but new cryptomarkets continue to appear to take up the slack, often with improved security. However, the proliferation of markets was not all good news for traders. Another weakness of the escrow system is that it involves trusting the market administrator, and this trust can be exploited. Several markets were involved in what were known as *exit scams* similar to those carried out by vendors. In an exit scam, a market trades as normal for a while, building up business, and then, at an appropriate moment when its escrow wallets are full, its owner simply cashes out the money they were holding for all the sellers. Trust in the market as a broker is destroyed, but the value of the multiple concurrent trades it was handling in escrow is considered worth it.

Cryptomarket technology has been evolving since 2013, however, and a solution to exit scamming of this form has been developed, known as *multi-sig*. The core concept is that an independent, verifiable algorithm acts as insurance for a trade. Money is transferred in to a multi-sig escrow system by the buyer, and can be transferred out if at least two of three cryptographic signatures authorise it, with the three parties being the buyer, the seller, and the market. As in a traditional escrow system, if the buyer receives the goods they can sign, and money goes to the seller. If the buyer disputes a transaction, they will not sign a transfer to the seller, and the market can decide which party is in the right and authorise a payment to either the buyer or the seller as appropriate. Unlike an ordinary escrow system, however, the market does not directly control transfer in multi-sig, and if the buyer and seller agree on a transaction it can go ahead without the market's say-so, preventing the market from being able to hold funds hostage or exit scam. This is an important step forward in market dynamics, and one that looks set to be significant for enabling safer—and therefore more lucrative—cybercriminal business.

3 OPTIONAL EXERCISES

These are suggestions for students who are particularly interested in the topic of cybercriminal economies. They are not assessed in any way. You don't need to complete the below to do well on the course.

3.1 *Further Reading*

On the topic of spam botnets, and in particular the market conflict between botnet operators, I recommend the book *Spam Nation* by Brian Krebs [8] – incidentally one of the best journalists in cybersecurity. The book carries a lot of interesting flavour, including the rather bizarre scenes where Vrublevsky, a top botnet operator, makes regular personal phonecalls to Krebs to talk about his day. A decent book on cryptomarkets is *Drugs on the Dark Net* by Martin [13], but this material ages quite quickly, and online resources and recent research articles are more useful for understanding the current state of play in the online drugs trade.

REFERENCES

References

[1] A. R. Rao and K. B. Monroe, "The effect of price, brand name, and store name on buyers' perceptions of product quality: An integrative review," *Journal of Marketing Research*, vol. 26, no. 3, pp. 351–357, 1989.

[2] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. M. Voelker, and S. Savage, "Show me the money: Characterizing spam-advertised revenue." in *USENIX Security Symposium*, vol. 35, 2011.

[3] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna, "The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns." *LEET*, vol. 11, pp. 4–4, 2011.

[4] G. Stringhini, O. Hohlfeld, C. Kruegel, and G. Vigna, "The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape," in *ACM Symposium on Information, Computer and Communications Security*, 2014, pp. 353–364.

[5] J. M. Rao and D. H. Reiley, "The economics of spam," *Journal of Economic Perspectives*, vol. 26, no. 3, pp. 87–110, 2012.

[6] C. Kreibich, C. Kanich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "On the spam campaign trail," *LEET*, vol. 8, no. 2008, pp. 1–9, 2008.

[7] J. Caballero, C. Grier, C. Kreibich, and V. Paxson, "Measuring pay-per-install: the commoditization of malware distribution." in *USENIX Security Symposium*, vol. 13, 2011.

[8] B. Krebs, *Spam nation: The inside story of organized cybercrime-from global epidemic to your front door*. Sourcebooks, Inc., 2014.

[9] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaker, V. Paxson, G. M. Voelker, and S. Savage, "Click trajectories: End-to-end analysis of the spam value chain," in *2011 IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 431–446.

[10] D. McCoy, A. Pitsillidis, J. Grant, N. Weaver, C. Kreibich, B. Krebs, G. Voelker, S. Savage, and K. Levchenko, "Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs," in *USENIX Security Symposium*, 2012, pp. 1–16.

[11] R. Thomas and J. Martin, "The underground economy: Priceless," *login*, vol. 31, no. 6, 2006.

[12] A. Haslebacher, J. Onaolapo, and G. Stringhini, "All your cards are belong to us: Understanding online carding forums," in *2017 APWG symposium on electronic crime research (eCrime)*. IEEE, 2017, pp. 41–51.

[13] J. Martin, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer, 2014.