A crime script analysis of the online stolen data market

Alice Hutchings[1], Thomas J. Holt[2]

Word count: 9,660

[1] University of Cambridge, Computer Laboratory, William Gates Building, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK
ph: +44 (0)1223 763660
email: ah793@cl.cam.ac.uk

[2] Michigan State University

Abstract

The purpose of this study is to better understand the online black market economy, specifically relating to stolen data, using crime script analysis. Content analysis of 13 English and Russian-speaking stolen data forums found that the different products and services offered enabled the commodification of stolen data. The marketplace offers a range of complementary products, from the supply of hardware and software to steal data, the sale of the stolen data itself, to the provision of services to turn data into money, such as drops, cashiers and money laundering. The crime script analysis provides some insight into how the actors in these forums interact, and the actions they perform, from setting up software to finalising transactions and exiting the marketplace.

Keywords

Online black market; Stolen data; Crime script analysis; Underground economy

Introduction

The Internet has facilitated new types of crime and enhanced more traditional forms of deviance (Holt & Bossler, 2014, Newman & Clarke, 2003, Wall, 2007). It has evolved from a communications system to a platform for all manner of trade, engendering the formation of markets that do not require buyers and sellers to interact in person. Alongside legitimate opportunities for commerce, online black markets can be found trading in drugs, firearms, skimming devices and pill presses (Barratt, 2012). In addition, a robust market has developed around digital commodities, such as stolen credit card details, other personal information, malware and exploit kits (Holt, 2013, Holt & Lampke, 2010, Motoyama et al. , 2011, Yip et al. , 2013). These marketplaces also provide information on how to commit offences and allow for the recruitment of co-offenders. They can also be used to advertise services such as writing code, developing spoofed websites, renting botnets, conducting denial of service attacks or laundering money.

Online black markets

Actors on online black marketplaces create challenges to our understanding of offender activities due to their relatively hidden nature, which is substantively different from market actors in real world illicit economies like drug or hawking markets (e.g. Cromwell & Olson, 2004, Jacobs, 1996, Johnson & Natarajan, 1995, Schneider, 2005). Actors may be less visible and harder to reach due to the mediating effects of the technology, which not only crosses geographical boundaries and eliminates distance, but also creates barriers in understanding the relationship between the people and the offences that they commit (Peretti, 2009). However, the artefacts that the marketplaces create, such as the posts between buyers and sellers, provide

data to understand how offences take place, and the offenders' attitudes toward one another and their practices (Holt, 2010).

There are a number of different types of stolen data sold on online black markets, with some more valuable than others. For example, ‘dumps’ are data read from the magnetic stripes of credit cards, which can be used for creating credit card clones (Holt & Lampke, 2010). Dumps with associated PINs are a valuable commodity, and are rarely offered for sale. Credit card data advertised as ‘CCV2’ includes credit card numbers and the card verification values, found on the back of the card, which are required to process online card-not-present payments. ‘Fullz’ include further information associated with the account, including data relating to the account holder, such as name, address, date of birth, and PIN. ‘COBs’ refers to ‘change of billing address’ data, providing enough information to allow an account to be hijacked, and the address details changed, such as online login credentials (Holt & Lampke, 2010). In addition to credit card details, products available on stolen data markets include eBay, PayPal, and bank accounts, stockmarket portfolios, as well as databases of email addresses (Holt & Lampke, 2010).

Hardware offered for sale on online black markets include those associated with stealing and subsequently using credit card data. Stolen or counterfeit identity documents, such as passports and drivers licences, can also be purchased on the marketplaces (Holt, 2013). Finally, individuals advertise services to acquire funds from stolen accounts, such as drop services, in which fraudulently purchased goods are received and exchanged for cash (Holt, 2013).

Advertised prices for stolen data may depend on the quantity of items to be purchased, the rarity of the items, the country of origin, the type of data, and further specifics (Holt et al. , 2013, Holt & Lampke, 2010). The advertised price may not

reflect the final price paid, as sellers offer discounts in order to attract customers and build trust within the market (Herley & Florêncio, 2010, Holt et al. , 2013, Holt & Lampke, 2010). The faceless nature of the market, however, increases the risk of loss for buyers, as a number of "rippers" or rip-off artists are present (Herley & Florêncio, 2010, Holt & Lampke, 2010, Thomas & Martin, 2006). Rippers typically obtain payment without providing the goods or service or sell the same data to multiple buyers (Herley & Florêncio, 2010, Holt & Lampke, 2010).

It is difficult to know how much of the information lost, whether through skimmers, data breaches, or stolen cards, is subsequently traded on the black market, and the financial impact on victims, banks or other parties (Herley & Florêncio, 2010, Holt et al. , 2013). This is because it is unknown how much of the data that are compromised are actively traded and used. Some figures are made available relating to reported card-present and card-not present credit card fraud on UK-issued cards, although it is noted that not all of these will include data that has been traded on the black market, rather than the financial institution. Also, it is not known if these data include fraud where losses are carried by the merchant or the cardholder. In 2013, card fraud totalling £450.4m was reported, an increase of 16% on the previous year. This was broken down into card-not-present payment fraud (£301.1m), counterfeit (skimmed/cloned) fraud (£43.4m), fraud on lost or stolen cards (£58.9m), card identity theft (£36.7m) and mail non-receipt (£10.4m) (The UK Cards Association, 2014).

Crime script analysis

Crime scripts outline the consequential steps and actions that are undertaken in order to prepare for, undertake, and complete a certain offence or offence type. Crime scripts borrow from cognitive science and the concept of ‘schemata’; knowledge

structures which allow individuals to organise their thoughts or understanding of events or social interactions so that they behave appropriately in response to others' behaviour (Cornish, 1994b). Scripts are learnt and undertaken by the offenders, similar to how actors learn their roles in a play.

Crime scripts include the events that occur prior, during, and after an event, or series of events. The universal script involves standardised script scenes or functions that are arranged in order, namely preparation, entry, pre-condition, instrumental pre-condition, instrumental initiation, instrumental actualisation, doing, post-condition and exit scenes (Cornish, 1994a). Cornish (1994a) notes that crime scripts are not prescriptive. Actors can also improvise when necessary to ensure their perception of success, which leads to innovation in relation to offending (Chiu et al. , 2011).

Crime script analysis is an emerging method for understanding crime types and developing crime prevention programs. By articulating what the script involves for a particular offence type, it identifies points of intervention. It has previously been applied to different crime types, such as child sex trafficking (Brayley et al. , 2011), robbery, auto theft and graffiti (Cornish, 1994a), and drug manufacturing (Chiu et al. , 2011), as well as crime 'actors', namely organised crime (Hancock & Laycock, 2010) and sex offenders (Beauregard et al. , 2007, Leclerc et al. , 2011). This project aims to extend the use of crime script analysis by applying it to a specific milieu, namely online black markets.

Method

Research question

With some notable exceptions (e.g. Herley & Florêncio, 2010, Holt, 2013, Holt et al. , 2013, Holt & Lampke, 2010, Mann & Sutton, 1998, Yip et al. , 2013), computer security researchers and vendors, who have a vested interest in the topic,

shape the discourse surrounding online black markets (e.g. Franklin et al. , 2007, Motoyama et al. , 2011, Ponemon Institute, 2014, Symantec Corporation, 2014). Their policy recommendations do not necessarily account for the social dynamics that shape market conditions or the process of offending, but rather automated techniques to disrupt actors. Such strategies may not be effective when implemented or fully account for the practices of offenders within the market.

Thus, the aim of this research project is to use crime script analysis as a tool to better understand the online black market economy. Specifically, this study attempts to identify what steps are required for offenders to interact and engage in these marketplaces. By understanding these processes, we can begin to understand and inform prevention opportunities for disrupting this underground economy. To that end, we utilize a qualitative analysis of posts from 13 Russian and English-language forums engaged in the sale of illegally acquired data and related services.

Design

Borrion (2013) notes that there are no established guidelines that inform how crime scripts should be created, particularly in relation to what data should inform crime scripts, or how they should be visualised, verified or validated. Crime scripts can be based on single crime events or individual offenders, or incorporate multiple accounts (Borrion, 2013). Multiple data sources can be used to create crime scripts including surveys or interview records (Beauregard et al. , 2007, Leclerc et al. , 2011) or reviewing court cases (Chiu et al. , 2011).

The data used for this research are 1,889 exchanges between buyers and sellers from a sample of 13 web forums where financial and personal information are bought, sold and traded. These forums also act as online discussion groups where individuals can present issues or discuss problems (Holt & Bossler, 2014). Each

forum is composed of threads, which are a series of posts that centre on a specific topic under a forum's general heading (Holt, 2010, Holt & Lampke, 2010, Motoyama et al. , 2011). Such threads are the primary source of data used in this analysis.

The sample of forums was developed via a snowball sampling procedure (see Holt, 2010, Holt & Lampke, 2010). Three English language forums were identified through Google.com using common terms in stolen data markets, including "carding dump purchase sale cvv" (Holt & Lampke, 2010, Motoyama et al. , 2011). Web links to other forums created a total sample of 10 Russian language and three English language forums. Eight of the sites sampled were publicly accessible, in that the entire site could be accessed by anyone in the general public. The five remaining sites required that an individual create a registered user account within the site to access the content of the sub-forums related to data sales. Registration-restricted forums are thought to differ from that of publicly accessible forums because they add a layer of insularity and protection from outsiders and the general public (Holt, 2010, Markham, 2011). Registration systems allow anyone to join by registering a username and password account with the forum. This is not as exclusive or secure as invitation only forums that completely exclude outsiders from access, though registration eliminates the potential for threads to be captured by search engines or identified easily by the general public (Holt, 2010, Markham, 2011).

Threads posted from carding or sales related sub-forums were captured to develop a substantive volume of posts. A certified Russian translator with substantive experience with technological jargon and forum communications translated the Russian language content from all forums. Due to the availability of the translator, convenience samples of 25 threads from each Russian forum were selected to capture the most recently posted items for sale in each site (see Table 1). Additional samples

of threads were translated from eight forums, particularly those that had active posting, to better assess the practices of actors and the network connectivity of participants.

Insert Table 1 Here

Analysis

The forum content was analysed using qualitative content analysis procedures. Coding of the data was "data-driven" or "open coding" (Gibbs, 2007: 45), in that it identified the key themes within the data; the universal script scenes put forward by Cornish (1994a). NVivo, a qualitative data analysis program, was used to classify and sort the data. The content provided in the results section have been provided verbatim, either as it appears in the original data or how it has been translated. On occasion, potentially identifying information has been removed, quotes have been reduced for reasons of parsimony, and sometimes explanations have been provided for the reader. The following results section outlines the script actions for actors on the online black markets. The results have been organised in accordance with Cornish's (1994a) universal script, namely preparation, entry, pre-condition, instrumental pre-condition, instrumental initiation, instrumental actualisation, doing, post-condition and exit scenes.

Preparation

Setting up the necessary client software and creating accounts

At the outset, participants in the market for stolen data need appropriate computer hardware, software, and user accounts to gain access to the Internet (computer, operating system, router, browser, an account with an Internet Service Provider, etc.). To successfully engage in transactions with buyers and/or sellers, individuals must also use software and accounts to communicate, such as webmail

accounts and instant messaging clients (for example, jabber, IRC or ICQ). Participants must also create accounts in on-line payment systems, such as WebMoney or Liberty Reserve, to facilitate the movement of money between buyer and seller.

It appeared that this process, as well as the process towards anonymity and security, is iterative. As actors become exposed to greater opportunities, they require specialised software or accounts for different online services. Also, the marketplace exposes actors to information about what software is required, with 'how-to' manuals and instructions available, particularly in relation to the topic outlined in the following section, steps towards anonymity and security. Therefore, exposure to the marketplace influences the types and sources of software that actors may download.

Steps towards anonymity and security

Actors could follow the essay-length tutorials posted about how to stay anonymous and secure. Fifteen such tutorials were found on five forums. These dealt with system configuration to avoid fraud detection systems and law enforcement attention, covering topics such as virtual machines, settings for operating systems and browsers, the use of socks proxies and anonymity networks such as Tor, considerations when selecting virtual private networks (VPNs), how to purchase hosting and domain services using stolen credit card credentials, how to wipe data and securely delete files, and how to encrypt files, email and chat services.

Physical security and anonymity was also addressed, with tutorials dedicated to receiving carded items through the use of drops at unoccupied houses and sending and receiving money. Some tutorials recommended obtaining a false passport, registering SIM cards to false identities, moving address on a regular basis, and advice was provided on how to travel long distances without being required to provide identification and how law enforcement agencies can use mobile phone data

to identify who was in a location at a certain time. One tutorial recommended that actors use unencrypted Wi-Fi, and/or crack WEP encryption, and move physical location every thirty minutes, although many advertisers took pride in announcing their near-constant web presence, so it is unlikely that these actors, at least, heeded this advice. Tutorials provided suggestions about how to avoid fingerprints being left behind, while another tutorial, titled "How to change your finger prints" provided a solution to those who had not followed this advice (source 7.2).

Some sellers advertised products and services aimed towards anonymity and security, such as dedicated servers (referred to as 'deds' or 'deddies'), VPN services, hosting services, socks proxies, hacked modems, scans of passports and other identity documents, as well as real and counterfeit passports (see also Holt, 2013). It appeared that there was some level of corruption involved on behalf of the providers. For example, the following is extracted from an advertisement for 'abuse-resistant' hosting and servers:

> *We have a good "roof"* [translator: officials providing protection] *with the authorities, which is a guarantee that we will not be subject to a "mask show"* [translator: police raid]. *If there are big problems, we have the possibility to solve them in advance and to prevent any idle time or deviations* (source: 5.1).

It appeared that not all the advice relating to anonymity and security was correct. For example, one advertisement falsely claimed that passports issued by the US Government contained GPS receivers. In addition, despite the advice provided, some marketplaces and actors do not follow 'best practice'. This related to the registration process to gain access to the sites, the choice of communication platforms for actors on the marketplace, and the use of encryption. For instance, forum content that can only be accessed through a registered account are thought to be more secure

than sites that can be indexed and accessed through search engine queries (see Herley & Florêncio, 2010, Holt, 2013, Motoyama et al. , 2011). Concerns were also raised about the security of ICQ, however this remained one of the most commonly advertised communication platforms.

Marketplace location

It was evident that there were a number of differences between marketplaces that influence actors' decisions about which to frequent. These included whether marketplaces were open or closed (e.g. Herley & Florêncio, 2010). The author of the following post argued that the types of discussions did not differ considerably across open or closed forums, but rather the type of actors who could be found on each:

> *There are many who live with illusions that the more private a platform is then the more private methods for earning there are there etc.as a person who knows a lot about such boards firsthand, I would like to say that many of these people are deeply mistaken* [...] *The main difference between a private board and a public one is the contacts with people* (source: 7.1).

The predominant language used was another differentiating factor between marketplaces. On the Russian marketplaces, actors who were not fluent or native speakers were admonished for grammatical errors. Some marketplaces were also dedicated to particular types of products or services, and even within the same product type there were specialities. For example, some marketplaces were known to offer credit cards from particular countries. Discussions on the forums about whether to use a particular site focussed on the presence of rippers, or rip-off artists who will cheat buyers by not sending products or services (Franklin et al. , 2007, Holt, 2013). Discussions also centred on whether there was a verification service for sellers, with some marketplaces having reputations for being 'ripper forums'. Should a forum have

a number of complaints, individuals may avoid engaging in transactions to minimise their risk of loss (Holt, 2013, Holt & Lampke, 2010).

It was evident that both buyers and sellers were active on multiple forums. In the following example, a buyer commented on the quality of a seller's products, claiming that the credit card data he sold had a low validity rate and he was aware that the seller sold under different names on other forums: *'different nicks on other forums. ofcourse not under it. many customers wrote about bad valid. if u exchange - no problem!'* (source: 2.1). Sellers who wished to advertise that they had established a good reputation named multiple marketplaces where they also traded. There was also evidence of displacement from one marketplace to another when forums were shut or closed down, or when individuals were banned.

Learning specialist knowledge

There were a number of different ways that were identified in which actors could obtain specialist knowledge. The first is through reading the free tutorials that were routinely posted by other actors, as discussed earlier. Ten advertisements on five forums were identified for paid tutoring, which covered specialist knowledge for a variety of topics, including carding, transferring funds, search engine optimisation, creating backdoors in software, and counterfeiting documents. In addition, two advertisements, were found on two separate forums, in which actors advertised their availability as apprentices in order to obtain specialist knowledge:

> *i want to try myself out in carding. I am a zero. but I work with hacked mail. if someone takes them for training the income will go to the teacher. that is I will work for training* (source: 13.1).

Four advertisers located on two forums offered technical support to their buyers, advising them on how to use their products, while 33 actors sought to obtain

specialist knowledge by posing questions on seven forums. Unsolicited advice posted in forums was also available for others to read and learn from. These were usually critical in nature, such as the following warning about attracting law enforcement attention by carding with colluding stores:

> *.....and later u and ur friends will be in prison...cause stolen dumps will be in 1 point (your store) someone auy will f**k ur partner in the store and you`ll be all arested.....its very simple sheme.....carding is very hard and don`t try the fortune with ur friends....take another places....different stores* (source: 2.3).

It was also suggested that specialist knowledge could be learnt by applying for employment at target companies, in this case a consumer credit reporting agency:

> *Another change that will be occuring within* [company] *is the closeure of all of their regional offices.* [The company] *is going to consolidate to one fixed location in* [city]. *The reason they are doing this is, and I quote, "To lover overhead costs, and also to increase security." So don't be too overly suprised if* [the company] *seems to be learning a few new tricks. The plan is to be completed within 2-3 years, with most of the outlying sites already closed. One nice note to this... If you live in* [city], *look in the want adds,* [the company is] *hiring Data Entry personnel... Hmmmm...* (source: 7.2).

In another post, a plan was outlined to either target employees who had knowledge of fraud detection software, or to gain employment at a company that used such software, in order to learn about how to avoid detection.

Entry

Learning marketplace language and rules

Marketplace rules were sometimes outlined within the forum, including rules relating to what should be included in advertisements, and what was forbidden (Holt,

2013). Forbidden behaviours included impersonating other people, leaving duplicate or fictitious reviews, or wrongly accusing others of being a ripper. Rules dictated that certain messages would be removed by moderators, such as reviews from users that had not previously been active on the forum; forum postings that were not related to the topic; or multiple messages from the author to promote their product. Failure to comply with the rules could result in posts being deleted, reputations being lowered or actors being banned from the marketplace (see Holt, 2013). There were also less formal outcomes, such as being criticised and rebuked by others on the forum.

In addition to marketplace rules, sellers often set out their own terms, such as if and when products would and would not be replaced. This primarily related to purchases of credit card data, such as not replacing credit cards that were declined or with little or no available funds (see Herley & Florêncio, 2010, Holt & Lampke, 2010). Some sellers advised buyers not to claim that their cards had 'died', as they checked them at the time of the transaction. This was despite there being discussion on the forums that such checkers were instrumental in 'killing' cards, as their use flagged fraud detection systems.

The language and slang used on the marketplaces was also valuable for members to understand the processes of the carding and black market community. The specialised argot included common jargon used in the financial industry, as well as unique slang, such as 'velveteen' for fake identification, and 'poison' for Yandex Money (the translator advised that the etymology of this possibly relates to the Russian words for money, 'деньги' or 'yandengi', and for poison, 'яд' or 'yad'). Those selling the goods would explain the terms, glossaries were posted as essays, and posts responding to queries would provide the meanings behind the vocabulary.

Pre-condition

Obtaining and manufacturing products to sell

Data, such as credit card details, were obtained through data breaches, using keyloggers, phishing, or by skimming credit cards either at point of sale or from ATMs:

> *I'M Sell freshly skimmed not hacked or generated, all Dumps are tested before sale. all dumps with original track1 and track2. Skimmed with camera and dial pad 100% working. No resales or fakes* (source: 2.3).

Products that could be used to obtain credit card data, such as skimmers, banking Trojans, fake point of sale systems, and keyloggers, were also offered for sale, and tutorials about obtaining data for fraudulent use were provided (Franklin et al. , 2007, Holt & Lampke, 2010, Motoyama et al. , 2011). Some services, such as web hosting, had been obtained through unauthorised access, with one seller posting that: '** Everything is hacked. Not make the confusion that this is paid hosting -)'* (source: 9.7).

Some sellers sometimes advertised that they had obtained their products themselves, while there were other indications that products and services were being resold. Some specified that the goods were supplied from elsewhere, while others posted advertisements indicating that their products had a margin for re-sale. Re-sold data increased the possibility that the same credentials had been sold to, and used by, other parties, and had a higher chance of being blocked by the time the buyer came to use them.

There was some evidence of collusion with legitimate providers, with the following advertiser indicated that he could obtain bank loans through corrupt bank staff, who would receive a cut:

Greetings! There is a topic in the [city]. *Thanks to connections at* [a bank], *it is possible to receive a loan for a large amount (the figure of 5 mln rubles was mentioned to me). Passengers are urgently needed! If it is a man, then a passport or military service card is needed, along with the lack of a criminal record and a credit history. Similar for women, but only a passport for docs. The terms of the offer are as follows: the bank takes 50% and we split the rest in half* (source: 6.1).

Instrumental pre-condition

Advertising products and services

Sellers advertised the products and services they were offering for sale, while buyers listed want ads if they were looking for specific products or services that may not be readily available. This included, for example, drops located in Germany or credit cards issued in Canada (source 2.2). Advertisers also ran promotions for their products, such as discounts for referrals, or holiday specials (see Herley & Florêncio, 2010, Holt & Lampke, 2010). Some marketplaces required payment for advertising, or for unverified advertisers. The following is an example of the advertising rules:

It is necessary to know:

Prices are shown in rubles. Without any sort of taxes.

The project's advertising department reserves the right to refuse to place advertisements without explaining the reasons.

Please note: there is strict 100% prepayment for the placement of advertising. By request, your banners may be placed using the system, which is smart and strong, so that's a you can track how your campaign is going in real time, or to the contrary, they can be placed "correctly." As you like it.

We except payments in Russian rubles, cash and electronic, and we may be

interested in barter, including advertising or goods. Write, we can discuss it (source: 6.1).

Undergoing verification procedures for products and services

Sellers could opt to have their products and services verified, or tested, by moderators (Holt, 2013). The following post explains the verification process for one of the forums:

> *Checking your goods will take place voluntarily or if the administration of the forum requires it. Checking of goods is done by* [ICQ number].
>
> *The check last from one to three days. After the check, the moderator guarantees that there will not be any stupid flames in the topic and that the quality of the goods will not be discussed. The moderator will write a review on this and close the topic. If a requirement to provide your product for testing is refused, you risk being banned, and your announcement will be erased. No money is taken for testing. You provide the product for the test in the same configuration in which you sell it* (source: 4.1).

If they passed this check (and there was no indication that those who had gone through the verification process had ever failed), then they would be listed as verified sellers. Although this process would, in theory, differentiate sellers from rippers, not every forum had verified sellers, even when the option to become verified was available. This was the case on one forum, which also had many claims that the sellers were rippers. At one stage, the moderator was urging sellers to become verified, and for buyers to only purchase from verified sellers, in an effort to clean up the marketplace and improve its reputation (source 2.2).

Some sites encouraged sellers to be verified by charging an advertising fee for those who had not gone through the process. Another advantage of being verified is

that others' claims that verified sellers were rippers were either deleted or admonished (Holt, 2013). This was demonstrated in the following case:

> [name] *is a verified seller on this forum and if you claim he's a cheater, then you can either report to the mods or prove how you were cheated.*
>
> *Disrespecting verified sellers on baseless accusations should be avoided.*
>
> *Respect this forum* (source: 8.1).

Verification was trusted more than other actors' feedback, as posts could be falsified to misrepresent the seller's business: '*don`t deal with this shit cause* [writer] *and seller are the same faces and ip`s* [IP address]*!!! be careful potential ripper!'* (source: 2.3).

Instrumental initiation

Exchanging law enforcement information

Actors exchanged information relating to law enforcement activities. This information related to which communication channels and individuals to avoid. Details of recent arrests were also shared: '*yeah! I`m fro* [country code] *and I knew admin of* [forum] *very well. was arested in middle of april and* [forum] *closed (((very good man (((*' (source: 2.3).

Occasionally concern was raised that an actor had disappeared, and it was evident that marketplace actors set out ways for trusted others to verify whether their accounts had been taken over (Holt & Lampke, 2010). Additional information exchanged about law enforcement investigations included aspects such as maximum harm that could be caused before an investigation will be initiated, and countries that were more likely to pursue fraud.

Negotiating and communicating

Advertisements contained contact details for those that were interested in their products or services. In some cases, multiple points of contact were offered, with options for ICQ, other messaging services, private messaging systems internal to the forums, and numerous email addresses. However, multiple communication channels provides multiple targets for account takeover by competitors and other adversaries: *'Dont talk to* [name 1] *on my icq .. My icq get hacked buy* [name 2] *... This is my new icq* [ICQ number]' (source: 9.15).

Although private communications were not accessible for this research, it was apparent that negotiation was encouraged in these exchanges (see Motoyama et al. , 2011). One tutorial provided advice on how to negotiate with vendors, and the sorts of questions to ask based on the type of product being purchased. Other sellers advised that they were open to negotiation for repeat customers and large orders (Holt & Lampke, 2010). In some cases, details of private communications were posted on the forums. IRC logs were posted in eight instances across four forums. This was usually done in response to a disputed transaction or to warn others about another actor who was believed to be a ripper (Holt, 2013).

Some advertisers specified how orders should be made. For example, in an advertisement for forged scans of documents, buyers were provided with a format, which included the: country; type of scan required; and information to be entered. Advertisers also laid out rules specifically relating to communication:

> *!!!!!! DO NOT email asking for tests, demos, freebies, telling me how you got scammed and crying and telling me I need to prove myself because your ass got ripped. I do NOT have time for noobs and cry babies. !!!* (source: 2.3).

Rules such as these were reinforced by tutorials that set out norms relating to acceptable communication. This was exemplified in the following post:

> *First of all. NEVER, I repeat, NEVER knock on the asy* [ICQ] *of people who are in the topic and do not write things like "Sorry for bothering you, I'm a novice and want to get into the topic tell me… (here there are many variations of what to say). I don't exclude that someone may actually say something, but 99% of those who actually work will have a desire to add you to their ignore list. People have no time, and even less desire to explain things to lazy and incompetent people* (source: 3.2).

Instrumental actualisation

Sending and receiving payment

Sellers accepted payment using a variety of providers: *'we are accept a lot of e-currency (wm* [WebMoney]*, lr* [Liberty Reserve]*, rbk* [RBK Money]*, yandex and others)'* (source: 2.1). Sellers also had differing requirements for different payment services, presumably based on factors such as the risk associated with using particular payment providers, or ease of access. For example: *'4. Minimum is $300 for WU* [Western Union] *or any amount for LR'* (source: 2.1).

Payment for products was usually required before delivery (Franklin et al. , 2007, Holt, 2013). This system of payment first differed in relation to service providers. For example, the following advertiser is listing drop and resale services, where the advertiser receives the carded items, fences them, and then retains their own payment (in this case, 50% of the resale price) before sending the remaining money to the person who commissioned them: *'I receive carded goods, resell and send you WU. I also can reship items. I work 50/50'* (source: 2.2).

In the following example, for email hacking services, the service was performed first, then payment received, following which the service provider would send the buyer the email password:

> *Payment is made through Webmoney or Yandex.Money, as well as through payment terminals/payment cards (more details on the site in the FAQ section). Payment only after the crack, we do not require any advances. Please note. You will get the password immediately after payment* (source: 5.2).

One advertisement, for a fake point of sales system that captured card details and PINs, sought reimbursement by way of a percentage of the data obtained, in addition to a payment for the system and shipping:

> *We are working only in %, we dont sell the pos without any %. So please dont bother asking to buy it off! The unit price is ONLY 1k euro+shipping(~200 euro)=~1200euro+8% for wu drops servise. IF YOU WORK WITH ESCROW SERVISE OF THIS FORUM COMMISSION FOR ESCROW WILL BE = 0%!!!. We really dont want your money, we want to get pin! The deal is, we take 40% and you get 60% of all pins!* (source: 9.4).

Some payment providers have a 'protection' service, whereby the seller can see that funds have been sent, but cannot receive them until the buyer provides a protection code or after a protection period. Many advertisers also indicated that they were worked with a guarantor or escrow service associated with a forum. Guarantors, for a percentage fee paid for by the purchaser, would receive the payment then would transfer the funds to the seller once both parties indicated that they were happy with the transaction (Herley & Florêncio, 2010, Holt, 2013). The following outlined the procedure for the escrow service provided by one of the forums:

The principle of insurance transactions:

1. Buyer pays Indemnitor amount of transaction and fees for escrow service. Reports icq number for which this sum is intended.

P.S. Under arrangement escrow fee may pay any member of transaction.

2. Escrow confirms receipt of money to another party.

3. The seller (service) provides direct product (or service) to another party to transaction without participation of Escrow.

4. After receipt and verification of goods (providing services) buyer contacts the Escrow and to announce completion of transaction.

5. Escrow pays money to seller (service) (source: 7.2).

However, the use of a guarantor did not necessarily guarantee that the funds sent by the buyer and intended for the seller would be received: *'Work through a guarantor, although the guarantor has completely disappeared, and hasn't answered for a month'* (source: 6.2).

Doing

Packaging goods

Packaging is a necessary step when sending physical goods, such as skimmers and plastics. However, there was little discussion found on the sites about how to package goods. This may be due to the preponderance of digital goods that are sent electronically, and there was some discussion about encryption in this regard. One exception was noted in the following excerpt from a tutorial, which discussed the pros and cons of sending items during holiday periods:

There are different times of the year that have advantages and disadvantages. Around holidays, especially Christmas can be good and bad. Christmas time is good because there are so many packages going through, it is hard to check

all the packages. On the other hand, it can also be bad because of terrorism, someone from a foreign country can be sending a mail bomb. So any packages that look suspicious will be opened. All in all people believe it is better to use the holiday season for sending packages. Ask the source how they package. It is a very good technique to wrap the package in wrapping paper and add a Christmas card that says "Merry Christmas". If your source does not use this technique, let him know about it (source: 7.2).

Transporting

Shipping products requires the buyer to provide the seller with a physical address:

Dumps can be sold on blank plastic but that will cost 200 uk pounds and a name and shipping address will be needed for delivery purposes all upon successful dispatch of card we will then send you tracking details so you can track your parcel online, delivery times vary per country (source: 2.1).

Shipping was the most popular delivery method listed for physical goods. The following advertisement indicated that it would only ship with specific companies: *'Shipping: WorldWide /TNT or DHL only !/'* (source: 2.3). There were a number of tutorials that provided recommendations for receiving items by post or courier, usually for the receipt of carded items. These covered topics such as delivery name, addresses to use, and signing for delivery. Few advertisements provided hand delivery, though those that did all appeared to be located in Eastern Europe. The following advertisements offered in-person delivery for plastics, fake identification, and cash from money laundering:

self pickup in Moscow, I say where to travel to, you take the ATM and give money, or delivery in Moscow within the Moscow Ring Road (source: 5.1).

*Delivery *in person* is possible through the courier services at your expense. Same-day deliveries possible Moscow* (source: 6.2).

You can get your percent both by webmoney, and with an ATM card also by meeting in person in Moscow (source: 13.3).

A number of advertisements for plastics in this region offered delivery using conductors on public transport:

Delivery: From the moment that you pay on the same day! Buses, Trains, mail (source: 4.1).

Delivery at your discretion ([translator: train] *conductor, courier service, bus, mail etc.)* (source: 4.3).

Delivery is carried out with the train conductors, bus or delivery service DHL/FeDex, the buyer's expense (source: 9.4).

Further enquiries with a Russian national revealed that delivery using train conductors could be faster than other delivery methods, and that this method was used not only for contraband, but delivering everyday items around the country. It appears that this method overcomes the difficulties with slow mail delivery in Moscow, which was complained about on the forums: *'the mail works horribly first-class delivery within Moscow - A WEEK'* (source: 6.2).

One advertisement for point of sale skimmers offered a technician to attend and install the devices in person, regardless of the location (source 8.8). Digital goods such as credit card information were sent over the Internet. One advertiser indicated that this could be by email, or could be downloaded using a link (source 2.3). Training services were also offered on these marketplaces. The following post, for search engine optimisation, specified the training would be delivered electronically: *The*

"set" includes the video materials, the necessary software and ICQ support, i.e. I will chew on any questions which interest you before and after the course! (source: 4.1).

Delivery for some services were specific to their nature, such as through financial accounts for money laundering. Similarly, telephone services must be delivered by phone, such as the following advertisement for 'calling services', used to overcome voice verification required for fraud detection systems:

> *Calling service men's and women's voices We offer calling of your drops , banks , shops , casi* [translator: casinos] , *WU, MG* [MoneyGram] *and many others. Price of a man's voice from 10 WMZ* [web money dollar units] , *a woman's from 12 WMZ . Languages English , German , Dutch , Polish and Serbian man's voice . Woman's voice - English . Calling and acceptance of calls* (source: 5.2).

Post-condition

Reputation management

There were a number of ways that sellers managed their reputations, to encourage new and repeat customers. The following advertiser sought recommendations from trusted forum users in exchange for free services:

> *Attention, we have a new promotion! FREE vpn throughout this week!How can you get it? It is very easy. If you have a sufficient number of messages on this forum (more than 200) and you are an active poster, then consider that the deed is half done. You only have to knock to the ICQ support service of* […] *and agreed to place a small message regarding our service under your signature* (source: 12.1).

Those who sold credit card information typically advertised that they would replace invalid (but not declined) cards within a set time period: *'replace all invalid*

within 24 hours' (source: 2.1). Credit card checkers were often used at the time of transaction to check the validity of a card. However, it appears that many card checkers would 'kill' cards, in that they would be subsequently flagged by fraud detection systems. The following post also raises the possibility that sellers could use this to their advantage and re-sell invalid cards. Some sellers posted that if their checker indicated that the card was valid at the time of transaction, then the card would not be replaced. However, in one case a buyer claimed that the seller's checker said that the card was still valid after another checker said that it was not:

> *Bought 1$ Cvv From Ur Site,I Checked On My Merchant For Just 1.99$ And It Said Card Not Valid Then Came Back To Ur Site And Checked On Ur Site Checker It Said Cvv IS VALID. TELL ME WHATS WRONG ?. UR CHECKER IS BAD ? PLZ FIX THAT* (source: 9.6).

Buyers who were unhappy after purchasing products or services would post claims that the particular seller was a ripper (Franklin et al. , 2007, Holt, 2013). In the some cases, the seller was 'doxed', or identified, for not providing the goods purchased. Ripper claims were disputed four times, across three different forums. It is possible that competitors may try and damage others' reputations by posting false information.

Buyers also posted positive reviews, although it was apparent that, at least in some cases, positive reviews were provided in exchange for a better price. Fake reviews, either claiming a seller is a ripper, or alternatively reviews written by or commissioned by sellers, were evidently a concern for forum moderators, with forum rules dictating that suspicious reviews would be deleted (see also Holt, 2013).

Exchanging currency

There were tutorials about how to exchange currency from one form to another, along with service providers who would do this on a fee-for-service basis. In addition, dumps sold on these forums could be encoded on plastics (also sold on the same marketplaces) and be transferred to money by hiring 'cashout services' (Holt & Lampke, 2010). Printed plastics are generally used to purchase goods for resale, or in the rare case where there is a PIN (due to their value, dumps with PINs are generally not advertised for sale), white plastics can be used to retrieve funds from ATMs. There were also many 'want' advertisements seeking such cashout services.

Individuals also listed advertisements, as well as want ads, for two specific methods of obtaining currency: 1) drops who received carded goods and resold them, and 2) mules who received money transferred into their bank accounts. These advertisements sometimes specified the country where the actors would need to operate and, in the case of mules, whether corporate or personal accounts were needed or provided. Bank accounts were occasionally offered for sale, for the receipt of money transferred using stolen banking credentials. Poker accounts were also advertised for sale for transferring money.

Sometimes it was revealed that cashing out involved collusion with merchants, as in the following example: *'i need any dump that has california bins....get back at me cos i can cashout and send u share in 20mins..i have a store guy thats on ma team'* (source: 2.3). Another service relating to the movement of funds was unblocking payment system accounts, such when they were suspended due to suspicious activity.

Exit

Laundering proceeds

Exchanging currency is not the same as money laundering. ‘Dirt’, or dirty funds, could be laundered using one of the myriad of services advertised on the forums:

> *A new WM-laundry has been opened for laundering funds "earned through blood sweat and tears" Cost of the services From 25% to 30% of the amount (the less the sum, the greater the %). Rate WMZ - -> Rubles (YaD* [Yandex Money]*, A etc.) from 26.5 to 28 rub. depending on the end system* (source: 5.2).

How dirt was cleaned was generally not discussed on the forums. Money launderers often also offered to exchange currency and transfer funds, however the percentage deducted for laundering was higher:

> *I've been working in encashment of clean money in the USA for 3 years now. Payment the next day. % depends on the amount from 8% to 15%. We can also for dirty* [money] *(45% to you)* (source: 6.1).

Discussion and conclusion

This study provides an overview of the script actions typically found when interacting in online black markets. Using a qualitative content analysis of three English and 10 Russian-speaking forums, we identified a number of actors and processes of the market through the crime script analysis. These included sellers, buyers, suppliers, moderators (who maintained order on the forums and applied the rules), administrators (who organised the platforms and the hosting of the actual forums), and teachers (who wrote tutorials and provided advice). These roles were not mutually exclusive, as one individual may take on multiple roles, such as seller and

buyer or administrator and moderator (Franklin et al. , 2007, Holt, 2013). Script actions included preparation, namely setting up the necessary client software and creating accounts, and learning about and taking steps towards anonymity and security. Actor also needed to select the marketplace/s that they wished to operate in, learn specialist knowledge, and learn the marketplace language and rules (Holt & Lampke, 2010).

Sellers were also required to obtain or manufacture, as well as advertise, the products they were to sell, and in many case, undergo verification procedures for their products and services (Franklin et al. , 2007, Holt & Lampke, 2010, Motoyama et al. , 2011). Information about law enforcement was also exchanged on the marketplaces, and actors negotiated and communicated using different channels. Once an agreement had been made, the next steps involved sending and receiving payment, packaging and transporting. Further actions included reputation management, exchanging currency and, finally, money laundering.

Taken as a whole, this study demonstrates the inherent value of crime script analyses to our understanding of on-line black markets specifically, and cybercrime generally. This study demonstrates that cybercrime markets enable offenders to affect a broader population of victims than is otherwise possible through real world crimes. Crime script analyses illustrates that while the techniques used to initially acquire personal information involve technically complex forms of hacking, the processes supporting the sale and misuse of information are similar to other forms of illicit markets off-line (e.g. Holt, 2010). Using crime scripts provides insights on the human actions and decision-making processes that lie behind cybercrime, demonstrating the points where situational crime prevention techniques may be used to complicate the process of offending and deter offenders (Newman & Clarke, 2003).

It is also important to note that while this study is based primarily on stolen data markets, some aspects of the crime script process may also be applicable to other online black markets, such as those that specialise in drugs or weapons (Barratt, 2012). In other aspects, the script will need to be altered based on the unique conditions of the market. For example, the process in relation to obtaining and manufacturing products to sell is likely to be specific to the type of products that are being traded.

The crime script developed here for online black markets differs from crime scripts that have been developed for other crime types. These differences include both the type of offences that are considered, as well as the platform on which they take place. For example, Brayley et al. (2011) identified how victims of child sex trafficking are found, groomed and abused by offenders. In contrast, the actors on the marketplaces considered in this research have little contact with victims, particularly in physical space. Instead, their targets are generally digital in nature, with a focus towards financial gain.

This script also differed from other crime scripts as it focussed on the marketplace itself, rather than on a particular offence type. For example, Chiu et al. (2011) examined the steps required to manufacture drugs in clandestine laboratories. Some of the steps were similar to those identified in this analysis, with obtaining precursor chemicals alike to obtaining and manufacturing products to sell on the black market. However, the focus on the marketplace itself allowed us to identify how the economy supported itself, with those selling products and services that are aimed at anonymity and security assist offenders who are entering the markets, while those who offer money exchange and laundering assist those exiting the market.

The data that are disposed of through online marketplaces are those that are compromised by the way of data breaches, and/or siphoned from individuals through the use of keyloggers, skimmers, and from phishing attacks (Franklin et al. , 2007, Holt & Lampke, 2010). The data can then be used to commit further offences, such as identity theft and fraud. Therefore, the sale of stolen data online acts as an intermediary between two other offences, obtaining and using the stolen data, by increasing demand for obtaining the data, and enabling it to be used fraudulently (see Herley & Florêncio, 2010, Holt, 2013). Disrupting these marketplaces may therefore have additional effects on other related offence types on- and off-line. Therefore, future work arising from this research will be to identify prevention and intervention methods to disrupt black market activities while minimising negative effects on legitimate Internet users (see Holt, 2013, Newman & Clarke, 2003).

This research has attempted to overcome the significant difficulties associated with this challenging area of research. However, a number of limitations in the research design are identified. First, as mentioned above, the results may not be generalisable to other marketplaces, including those that are invitation-only. The second limitation is the validity of the data upon which the research is based. It is possible that law enforcement or others interact on the marketplace for investigative or research purposes. Some of the threads observed may relate to those posing as offenders, rather than those who actually engage in illegal or antisocial behaviours (see Holt, 2010).

Finally, this paper has attempted to be relatively technology-agnostic, without specialising on particular tools. For example, there appears to be a change in the types of payment providers that are used on black markets as some close down and others become available (e.g. Holt, 2013). While some providers, software and tools have

been referred to in the data, these may be thought of more generally in relation to the provision of enabling services, rather than specific brands or organisations.

Funding

This work was supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131, to A.H.]; and the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice [2010-IJ-CX-1676, 2010, to T. H.]. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

Acknowledgements

The work would not have been possible without the invaluable assistance of Richard Clayton and Ross Anderson.

References

BARRATT, M. J. (2012), 'Silk road: eBay for drugs'. *Addiction* 107/3: 683-683.

BEAUREGARD, E., PROULX, J., ROSSMO, K., LECLERC, B. & ALLAIRE, J.-F. (2007), 'Script analysis of the hunting process of serial sex offenders'. *Criminal Justice and Behavior* 34/8: 1069-1084.

BORRION, H. (2013), 'Quality assurance in crime scripting'. *Crime Science* 2/1: 6.

BRAYLEY, H., COCKBAIN, E. & LAYCOCK, G. (2011), 'The value of crime scripting: deconstructing internal child sex trafficking'. *Policing* 5/2: 132-143.

CHIU, Y. N., LECLERC, B. & TOWNSLEY, M. (2011), 'Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention'. *British Journal of Criminology* 51/2: 355-374.

CORNISH, D. B. (1994a) 'Crimes as scripts', *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*, pp. 30-45: Florida Statistical Analysis Center, Florida Criminal Justice Executive Institute.

CORNISH, D. B. (1994b),'The procedural analysis of offending and its relevance for situational prevention'. in R. V. Clarke, ed., *Crime prevention studies*, 151-196, Monsey: Criminal Justice Press.

CROMWELL, P. F. & OLSON, J. N. (2004), *Breaking and Entering: Burglars on Burglary.* Thomson/Wadsworth.

FRANKLIN, J., PAXSON, V., PERRIG, A. & SAVAGE, S. (2007) 'An inquiry into the nature and causes of the wealth of internet miscreants', *ACM Conference on Computer and Communications Security (CCS), 375– 388*.

GIBBS, G. (2007), *Analyzing Qualitative Data.* London: SAGE Publications Ltd.

HANCOCK, G. & LAYCOCK, G. (2010),'Organised crime and crime scripts: prospects for disruption'. in K. Bullcock, R. V. Clarke & N. Tilley, eds., *Situational prevention of organised crimes*, 172-192, New York: Taylor & Francis US.

HERLEY, C. & FLORÊNCIO, D. (2010),'Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy'. in T. Moore, D. Pym & C. Ioannidis, eds., *Economics of Information Security and Privacy*, 33-53: Springer.

HOLT, T. J. (2010), 'Exploring strategies for qualitative criminological and criminal justice inquiry using on- line data'. *Journal of Criminal Justice Education* 21/4: 466-487.

HOLT, T. J. (2013), 'Exploring the social organisation and structure of stolen data markets'. *Global Crime* 14/2-3: 155-174.

HOLT, T. J. & BOSSLER, A. M. (2014), 'An assessment of the current state of cybercrime scholarship'. *Deviant Behavior* 35/1: 20-40.

HOLT, T. J., CHUA, Y.-T. & SMIRNOVA, O. (2013) 'An exploration of the factors affecting the advertised price for stolen data', *eCrime Researchers Summit (eCRS), 2013*, pp. 1-10: IEEE.

HOLT, T. J. & LAMPKE, E. (2010), 'Exploring stolen data markets online: products and market forces'. *Criminal Justice Studies* 23/1: 33-50.

JACOBS, B. A. (1996), 'Crack dealers and restrictive deterrence: Identifying narcs'. *Criminology* 34/3: 409-431.

JOHNSON, B. D. & NATARAJAN, M. (1995), 'Strategies to avoid arrest: Crack sellers' response to intensified policing'. *American Journal of Police* 14/3/4: 49-69.

LECLERC, B., WORTLEY, R. & SMALLBONE, S. (2011), 'Getting into the script of adult child sex offenders and mapping out situational prevention measures'. *Journal of Research in Crime and Delinquency* 48/2: 209-237.

MANN, D. & SUTTON, M. (1998), '>> NETCRIME More Change in the Organization of Thieving'. *British Journal of Criminology* 38/2: 201-229.

MARKHAM, A. N. (2011),'Internet research'. in D. Silverman, ed., *Qualitative Research: Issues of Theory, Method, and Practice*, 111-127, Thousand Oaks, CA: SAGE Publications.

MOTOYAMA, M., MCCOY, D., LEVCHENKO, K., SAVAGE, S. & VOELKER, G. M. (2011) 'An analysis of underground forums', *2011 ACM SIGCOMM conference on Internet measurement*, pp. 71-80, Berlin, Germany: ACM.

NEWMAN, G. & CLARKE, R. V. (2003), *Superhighway Robbery: Preventing E-commerce Crime.* Devon: Willan Publishing.

PERETTI, K. K. (2009), 'Data breaches: what the underground world of carding reveals'. *Santa Clara Computer & High Tech. LJ* 25: 375-413.

PONEMON INSTITUTE (2014), *Cost of Data Breach Study: Global Analysis.* IBM.

SCHNEIDER, F. (2005), 'Shadow economies around the world: what do we really know?'. *European Journal of Political Economy* 21/3: 598-642.

SYMANTEC CORPORATION (2014), *Internet Security Threat Report.* Mountain View: Symantec Corporation.

THE UK CARDS ASSOCIATION (2014), *Scams and computer attacks contribute to increase in fraud, as total card spending rises.* London: The UK Cards Association.

THOMAS, R. & MARTIN, J. (2006), 'The underground economy: Priceless'. *;Login* 31/6: 7-16.

WALL, D. S. (2007), *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

YIP, M., WEBBER, C. & SHADBOLT, N. (2013), 'Trust among cybercriminals? Carding forums, uncertainty and implications for policing'. *Policing and Society* 23/4: 516-539.

Table 1: Forum Descriptive Statistics

Forum	Language	# of Threads	First Post	Last Post
1	RU	55	12/31/10	7/21/11
2	ENG	128	12/1/10	2/23/11
3	RU	6	10/17/10	7/16/11
4	RU	144	10/3/09	12/25/2011
5	RU	89	6/6/08	12/11/11
6	RU	48	2/5/09	11/14/11
7	RU/ENG sub	202	12/26/10	7/9/11
8	ENG	590	4/1/09	11/1/11
9	RU/ENG sub	312	4/1/11	7/21/11
10	RU	35	4/10/10	3/7/11
11	RU	60	5/9/07	2/25/12
12	RU	71	11/7/07	11/9/11
13	RU	153	6/6/07	7/25/11