Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world"

Benoît Dupont[1], Anne-Marie Côté[1], Jean-Ian Boutin[2], and José Fernandez[3]

American Behavioral Scientist, 2017, Vol. 61 (11), pp. 1219-1243, Reprinted by permission of SAGE Publications, http://journals.sagepub.com/doi/abs/10.1177/0002764217734263.

Abstract

This article explores the social and market dynamics of Darkode, an invitation-only cybercrime forum that was dismantled by the FBI in July 2015 and was described by a U.S. Attorney as "the most sophisticated English-speaking forum for criminal computer hackers in the world". Based on a leaked database of 4788 discussion threads, we examine the selection process through which 344 potential new members introduced themselves to the community in order to be accepted into this exclusive group. Using a qualitative approach, we attempt to assess whether this rigorous procedure significantly enhanced the trust between traders, and therefore contributed to the efficiency of this online illicit marketplace. We find that trust remained elusive and interactions were often fraught with suspicion and accusations. Even hackers who were considered successful faced significant challenges in trying to profit from the sale of malicious software and stolen data.

Keywords

Internet, malicious hackers, malware, illicit online markets, trust

Corresponding Author

Benoît Dupont, CICC / UdeM, Pavillon Lionel Groulx, CP 6128 succursale Centre-Ville, Montreal (QC) H3C 3J7, Canada
Email: benoit.dupont@umontreal.ca

[1] Université de Montréal, Montreal, QC, Canada
[2] ESET, Montreal, QC, Canada
[3] École Polytechnique de Montréal, Montreal, QC, Canada

Introduction

On 15 July 2015, the FBI and the U.S. Department of Justice announced the takedown of a computer hacking forum known as Darkode, which led to the indictment of 12 suspects and the arrest of 70 other members across 20 countries (Zetter, 2015). U.S. Attorney David Hickton described Darkode as "… one of the gravest threats to the integrity of data on computers in the United States and around the world and … the most sophisticated English-speaking forum for criminal computer hackers in the world" (FBI, 2015). Europol's slightly less dramatic media release stated that Darkode was "the most prolific English-speaking cybercriminal forum to date" (Europol, 2015). Darkode was certainly not the first online illicit marketplace to attract the interest of law enforcement agencies and to be taken down following a long-lasting infiltration operation (Ablon et al., 2014), but the fact that it was accessible only by invitation and claimed to cater to a small but exclusive community of elite malicious hackers makes it uniquely interesting for researchers.

Most of the scientific literature on malicious hackers and the illicit digital marketplaces on which they converge to exchange knowledge, find new co-offenders, and trade malicious malware, criminal services, and stolen data relies heavily on data culled from easily accessible public or semi-public online forums. Lacking technical skills and criminal contacts, aspiring malicious hackers end up on forums that are easy to find and welcome anyone; these forums are also easier for academics, bound by the rigorous constraints of research ethics boards, to study. Unfortunately, most such forums suffer from a structural trust deficit (Dupont et al., 2016) and serve largely as fertile hunting grounds where cunning "rippers" take advantage of the gullibility of novices (Herley and Florêncio, 2010). The most experienced, skilled, and successful hackers ply their trade on closely guarded invitation-only forums, which are almost impossible for academics to study ethically, making it extremely difficult to learn more about the dynamics of these thriving marketplaces. Most of the knowledge about them comes from journalistic investigations, which emphasize the human interest aspects of this rapidly expanding underground economy (Glenny, 2011; Poulsen, 2011; Krebs, 2014) and are understandably more interested in chronicling the experiences of high profile hackers than providing a comprehensive analysis of the nature and structure of their illicit exchanges. This knowledge gap is regrettable, as the volume and impact of online harms are clearly on the increase according to the latest statistical data available from the U.K., which is the only jurisdiction that has added online crimes to its victimization survey (Office for National Statistics, 2016), and now represent the main form of criminal offence against both organizations and individuals.

However, on rare occasions highly secured illicit online forums are hacked by competitors or vigilantes and the content of these forums is publicly released. On 1 April 2013, a French blogger using the alias "Xylitol" released a cache of 4788 files taken from Darkode that exposed the forum's membership, products and services for sale, and various discussions over the previous four years between some of the world's most prolific malicious hackers and programmers. This article provides the first analysis to date of these files and examines the specific social and business dynamics of what was for a time a very active digital convergence setting for successful online offenders. The recourse to such "found" data does raise some ethical and data-reliability issues (McCoy et al., 2012). However, although it's impossible to entirely exclude the possibility that some of the files were forged in an effort to implicate particular members, the efforts

required to generate hundreds or thousands of fake discussion threads would be disproportionate to the expected benefits. Furthermore, a highly respected journalist with an intimate knowledge of the cybercrime underground reviewed the files and found no reason to question their reliability (Krebs, 2013a). Ethical use of this data was greatly facilitated by their format, which ensured that metadata or other types of identifying information could not be inadvertently obtained and shared. As well, Darkode members used only aliases and were extremely prudent in their operational security practices, making it impossible to guess their real identity, except in the case of those who were arrested in the FBI takedown and named in the indictments that followed.

We were particularly interested in the Darkode selection process, during which potential new members introduced themselves to the community as a first step to being accepted into this exclusive group. Using a qualitative approach, we attempted to assess whether this apparently stringent procedure significantly enhanced trust between traders, thereby contributing to the efficiency of this illicit online marketplace. In the first section, we provide an overview of the criminology and computer science literature on online illicit markets and the trust dilemmas afflicting them. In the second section, we give a short history of Darkode before describing in a third section the data we used and the analyses we performed. The fourth section examines the presentational strategies of 344 candidates attempting to join the forum and the outcome of these applications. The relevance of personal connections, past experiences, technical skills, and business interests, including products and services available for sale, are discussed. Finally, based on two case studies, a fifth and final section casts new light on the challenges faced by cybercrime entrepreneurs dealing with demanding customers who do not hesitate to leak the malware they have just purchased to the broader hacking community, significantly eroding the profitability of such endeavors.

Malicious hackers, illicit markets, and trust as a cooperative enabler for criminal achievement

While most criminal online markets operate as virtual open-air bazaars, with very low entry barriers in an attempt to attract anyone with an interest in buying or selling malware or stolen information, a few of them have adopted a different model and function as private clubs, accessible to members by invitation only (Holt, 2013). A broad overview of what we know about online illicit markets and their failures is needed to understand why this counter-intuitive approach is sensible.

The main purpose of an online illicit market is to connect sellers and buyers to allow them to trade in the broad range of products and services that allow them to execute and profit from their criminal projects. The global nature of online crime generates tremendous opportunities for malicious hackers by providing access to an unprecedentedly large pool of victims (both machines and humans). However, identifying and recruiting co-offenders who master the highly specialized technical skills required to carry out complex digital theft and fraud schemes represents a challenge. To connect the supply and demand of such expertise, online illicit markets offer virtual convergence settings where offenders can congregate, develop rapport, and forge profitable business ties with accomplices (Felson, 2003; Soudijn & Zegers, 2012; Leukfeldt et al., 2016a; Macdonald & Frank, 2016). Online illicit markets operate on technological platforms that include Internet Relay Chat (IRC) channels (synchronous), web

forums (asynchronous), and, more recently, the Onion Router (Tor) network (Décary Hétu and Giommoni, 2016). Transactions are often completed via private messaging tools to ensure the confidentiality of negotiations (Holt, 2013; Yip et al., 2013). These platforms also play a significant knowledge transfer function (Soudijn & Zegers, 2012), replacing prisons as the "university for cybercriminals" (Leukfeldt et al., 2016a).

Over the past few years, a growing body of knowledge has begun to provide a better understanding of these markets' structure and social organization, with a particular emphasis on forums. Yip et al. (2013a; 2013b) identified four main features that make forums so attractive to cybercriminals: formal control and coordination mechanisms, social networking opportunities, and methods to help mitigate both identity and quality uncertainty. Holt and Lampke (2010) used qualitative analysis to describe the types of information and services for sale on such markets, the price and quantities available, and the forces (communications, price, quality, and service) that influence transactions. Holt (2013) applied the organizational framework developed by Best and Luckenbill (1994) to show how the organizational complexity of cybercrime forums varies, ranging from informal groups of colleagues to more structured organizations, and how they facilitate a division of labor. Several researchers have also used social network analysis (SNA) methodologies to understand the structural properties of cybercrime forums and the ties that bind their members, often using these insights to suggest optimized disruption strategies (Lu et al., 2010; Motoyama et al., 2011; Yip et al., 2012; Monsma et al., 2013; Décary-Hétu and Laferrière, 2015; Macdonald and Frank, 2016). Finally, a few researchers have applied the crime script analysis approach, used by situational crime prevention scholars to break down the flow of actions involved in committing an offence, to the online settings of cybercrime forums (Soudijn and Zegers, 2012; Hutchings and Holt, 2015; Hutchings and Holt, 2016), shifting the focus of disruption strategies from individual nodes to specific tasks and functions.

One of the major features of cybercrime forums is the inherent mistrust that characterizes interactions between members who trade in deception. Herley and Florêncio (2010) were among the first to express skepticism about the profitability of the most common forms of hacking and online fraud, noting that illicit markets are crowded with rippers – market participants who do not deliver the products and services for which they have been paid, or who supply products of a lesser quality than what they had promised buyers. Rippers are ubiquitous on illicit markets and create uncertainty and paranoia that hinders the natural flow of transactions. There may be a high level of activity on open online illicit markets, but the level of activity does not ensure great economic performance. Such markets have been compared to the famous market for lemons first theorized about by Akerlof (1970), where information asymmetry between buyers and sellers distorts the prices and produces suboptimal outcomes for honest traders.

In order to facilitate detection of rippers so that they can be excluded from cybercrime forums, administrators have implemented a broad range of controls, regulations, and reputation management tools inspired by the solutions developed by e-commerce platforms (Lusthaus, 2012; Soudijn and Zegers, 2012; Yip et al., 2013b; Holt et al., 2015). These risk-reduction strategies are intended to buttress trust and make markets more efficient, but preliminary evidence from the world's largest hacking forum indicates that they do not translate into these markets as easily as had been hoped (Dupont et al., 2016). It has been suggested that

the most effective way to overcome this trust dilemma would be to either raise the cost of participation in order to deter rippers (Afroz et al., 2013) or, more drastically, to limit membership to a small group of reliable participants (Yip et al., 2013b). A limited number of cybercrime forums have adopted an exclusive model (Ablon et al., 2014). While we know relatively little about the economic performance of cybercrime forums, the criminal achievements of those who patronize them (Franklin et al., 2007; McCoy et al., 2012; Allodi et al., 2016; Décary-Hétu and Leppänen, 2016; Holt et al., 2016), or what makes these markets sustainable (Afroz et al., 2013), it certainly seems possible that a hand-picked group of skilled and experienced hackers would trade much more effectively and efficiently than a large community of self-selected members comprised mainly of novices or individuals with very limited technical and monetary skills. Most of the available literature on online illicit markets has relied on empirical data collected from publicly accessible forums, with a smaller sample of studies using registration-only forums, which require a self-selected password and are not indexed by mainstream search engines (Holt, 2016). To the best of our knowledge, no research has yet analyzed the admission and market dynamics of an invitation-only forum, the main contributions of the present article, which discusses data obtained from Darkode.

A short history of Darkode

In the absence of official records and reliable archives, documenting the history of online illicit forums is a challenge. Their administrators generally try to evade the attention of outsiders and law enforcement investigators by limiting access to content posted by members and avoiding indexing by search engines through the use of an industry standard known as the Robots Exclusion Protocol (or 'robots.txt' command), which lets search engines know that the collection of data from some webpages should be avoided (Koster, 1996), or by using password-protected landing pages that block access to a website. Unless a researcher has been granted access to an illicit forum from early in its existence or has been able to retrospectively and comprehensively download its contents, she must rely on third parties, such as journalists, security bloggers, and eventually hackers themselves, in any attempt to understand the reasons and conditions that led to the creation and development of such online criminal marketplaces.

According to such third-party sources, Darkode was launched in March 2008 by a Slovenian hacker named Matjaž Škorjanc and an American hacker named Daniel Placek. Škorjanc had coded and marketed the Mariposa botnet, a powerful piece of malware that at its peak phase managed to enslave close to 13 million compromised computers (BBC, 2013), while Placek was more interested in programming credential-sniffing software (Hrodey, 2015). According to Placek's very candid recollection, their intent was to: "Start a little community, invite-only … where we could get some like-minded people together and really just talk [about malicious] code … We don't want the script kiddies, people who are just using these tool but don't really understand them. Let's get the people who are really making the stuff … We started it up and invited a few people that we already knew … chatting about code, sharing a little bit of code … Initially, it was a pretty small group, less than 25. Day one, it was five people or something, and it grew over time. We talked about the projects we were working on, we talked about ideas, talked about some of the different technologies" (Placek, 2016).

The community benefited indirectly from takedowns of a number of public cybercrime forums

that left hackers with limited options for forums to trade their wares. The fact that Darkode had adopted an invitation-only policy became an attractive feature that gave it a veneer of exclusivity and contributed to a quick rise in popularity. Simultaneously, existing members decided to bring in buyers. In Placek's words, "we had these people who were creating things, and some of them had some customers that they worked with already, and they wanted to bring them on there and be able to sell to them through that platform as well" (Placek, 2016). Efforts were made to divide the site into sections that were accessible to members according to their level of technical expertise, with some sections reserved for the programmers who were most skilled at developing malware. On his own admission, Placek was not as successful an entrepreneur as his associate Škorjanc, who managed to sell his botnet code to a few hundred people for $500 to $2,000 apiece (Krebs, 2015). Both of them disengaged from the forum in 2010: Placek a few months before his arrest by the FBI (his arrest was not made public until 2015, and he collaborated with the law enforcement agency during those five years) (Hrodey, 2015), and Škorjanc following his capture by the Slovenian police in July 2010 (FBI, 2010).

A Swedish hacker named Johan Anders Gudmunds, who used the online aliases of Mafi, Crim and Synthet!c, took over the forum's administration responsibilities, with the help of another member who used the alias Fubar. Both hackers had developed and were selling malware that allowed others to build and operate botnets (the Crimepack exploit kit for Crim and the Ngrbot malware for Fubar) (Krebs, 2015). The forum's continuous growth attracted successful Russian hackers such as AlexUdakov, Gribodemon, or Paunch, who had developed popular and easy-to-use malware packages such as the Phoenix exploit kit, the SpyEye trojan, or the Blackhole exploit kit. But this high profile membership also attracted the attention of law enforcement investigators and security researchers, who infiltrated the forum to collect intelligence, creating a sense of paranoia among members and leading its administrators to aggressively ban suspicious accounts and tighten admission criteria (MalwareTech, 2014; Krebs, 2015).

In January 2013, a new administrator, nicknamed Sp3cial1st, who had been one of the forum's early members, had done business with a significant share of the forum, and had a reputation for spending a great many hours online, was voted in. He proceeded to vastly expand the forum's membership by advertising on beginner forums such as HackForums and by sending unsolicited emails to the members of old hacking forums (Xylitol, 2013; MalwareTech, 2014). This broad recruitment drive attracted a more diverse set of hackers to Darkode, including some who actively sought the media's attention through very high profile attacks. The Lizard Squad crew, which gained notoriety in December 2014 for its Distributed Denial of Service attacks against Microsoft Xbox and Sony Playstation servers, wrecking Christmas for millions of video game players, is representative of this new wave of Darkode members (Turton, 2015).

As its status rose among elite hackers, Darkode was regularly infiltrated by security professionals, who used their access to monitor members and their dealings. On 1 April 2013, a French white-hat hacker known as Xylitol, who had established a reputation as a technically sophisticated vigilante bent on disrupting cybercrime activities, released most of the forum's contents after one of its members used Xylitol's handle to conduct illegal business online (Krebs, 2011; Xylitol, 2013; Pauli, 2013; Hrodey, 2015). Xylitol's leak did not, however, prevent Darkode from remaining a thriving marketplace until its takedown by the FBI. Following the forum's takedown in July 2015, Sp3cial1st, who had avoided arrest, attempted to move the forum to a more secure infrastructure that relied on the obfuscation technologies of the dark web, such as

the Tor network, but the resurrected forum was poorly secured and failed to regain the trust of past members (Kharouni, 2015).

Using hacker leaks to study cybercrime

The data leaked by Xylitol provides a unique window into the sustained interactions of a community of very active and undeniably malicious hackers. Although the material was initially meant to expose and embarrass the members of this community, such a leak also provides researchers with high quality second-hand material that they would have difficulty collecting themselves—for both technical and ethical reasons—enabling them to understand the social and business dynamics of these groups. The dataset consists of 4788 screenshot files extracted from the forum's discussion threads and covers a five-year period, from 2009 to March 2013. It amounts to 819.69 megabytes (Mb) of data and can be downloaded from http://darkode.cybercrime-tracker.net. The files are organized in folders that reflect the structure of the forum's sections: posts include a membership list, products for sale, transaction reports about new products offered to the community, malware analysis reports, tutorials and programming tips, questions about specific problems, and a "Hall of shame" section where complaints were aired and conflicts were adjudicated by the administrators. This material is in the Portable Network Graphics (PNG) file format, so we attempted to batch process the database using powerful Optical Character Recognition (OCR) programs and customized solutions offered by computer science colleagues. Unfortunately, none of these automated techniques for content analysis were successful, forcing us to manually parse and code every image to extract the information it contained. Figure 1 illustrates the appearance of a typical screenshot, where only the file name is searchable. Each discussion thread contains multiple contributions posted by forum members whose alias, membership level, accession date, number of posts, reputation level, and location are published, although this last piece of information is notably unreliable. Note for example Mafi's location in Figure 1's first message: "Siberia, Igloo 36b", although he was eventually found to live in Sweden.

[INSERT FIGURE 1. ABOUT HERE]

For this part of our study, after carefully considering the quantity of posts available for analysis, the resources at our disposal, and the need to better understand the membership of this forum and its structure, we decided to focus initially on a subset of discussions that seemed to provide the best information to effort ratio: the introductions provided by aspiring new members. As discussed above, Darkode was an invitation-only forum. Once a prospective member had secured an invitation from one of the forum's existing members (who usually received an allowance of two invitations but could always replenish them by asking the administrators), he (as members were exclusively male) was admitted to the unverified section (Level -1) where he had to complete the verification and accession process by introducing himself to the community. As outlined in a post by Sp3cial1st from July 2010 (see Figure 2), introductions were intended to highlight the skill set, recent experience, ongoing activities, and motivations of an applicant. As well, candidates usually disclosed who had invited them to join the forum. For people who had no prior contacts in the community, an interview with trusted

members (Level 1 or 2 in the forum hierarchy) was also required. Each introduction was then commented on by existing members, who assessed the value of the candidate and voted to accept or reject the application. These comments often reveal prior collaborations and business exchanges between the candidate and established members, usually carried out on other underground forums. The introductions and the discussions that follow thus operate as a typical recruitment interview where a hacker uses his introductory message to provide a criminal CV that must convince potential co-offenders of his technical and business worth, while the resulting evaluations reveal prior criminal links, as well as the current preferences and needs of this large community of elite hackers.

Once accepted, new members (designated as Fresh Fish, probably in reference to a slang term used since the mid-18th Century to describe new prison inmates and popularized in the 1994 movie The Shawshank Redemption) gained access to Level 0 of the forum, where they could buy certain products and participate in various conversations. After they earned the trust of their peers, they were admitted to Level 1, where business dealings were less restricted, and eventually to Level 2, open only to highly trusted members such as administrators and influential hackers. In one of the administrator's own words, "the point of the level system is to be less strict on the invitation, where more people will have a chance to contribute and eventually become level 1" (Mafi), while at the same time shielding the most sensitive contents and transactions from new entrants whose trustworthiness was uncertain. However, in a thread discussing a limited leak by Xylitol in October 2012, one of the commenters reminded his peers that such a rigid hierarchy proved hard to enforce in practice when participants wanted to expand their market: "everyone sell their product's into the level 0 lol … level 1/2 users must stop making sales into the level 0 system and to start finally to be active into the level 1" (Pwdot). As the same user stated more bluntly in a follow-up post, "the main idea was to separate the good members from the dumb ass and to keep secure the whole forum ... but instead of that, everyone moved into level 0 keeping dead the level 1 section."

[INSERT FIGURE 2 ABOUT HERE]

The introduction section of the available data contains 344 applications (476 screenshots) from new prospects or former members who had remained inactive for extended periods of time and had to be re-accredited by the group. The coding was done manually by two research assistants who used a codebook designed by the principal investigator and reviewed each other's work for consistency. Ambiguous material was discussed with the principal investigator and the codebook edited accordingly to ensure internal homogeneity (Saldaña, 2009: 21). Each of the 344 applications (see Figure 3 for an example) was processed as a single event and entered into a coding database where we recorded the alias of the candidate, the member who sponsored him, his participation in other forums, the technical skills he claimed he had mastered, his business interests (for example, whether he was a seller or a buyer), his motive in joining the forum, and the products he was offering to trade with other members. We also coded each response to these initial introductions, in which existing members welcomed candidates, asked them questions or to clarify specific skills or experience, or publicly discussed the potential value that a prospective member would bring to the community. For each comment, we recorded the nickname of each member who participated in the evaluation

process, the nature of his assessment (what had triggered a positive or negative comment), as well as the general outcome of the application. Overall, there are 404 discrete aliases in our database (344 candidates and 60 "historical" members). In other words, we tried to simultaneously capture the qualitative and quantitative dimensions of these interactions in order to understand how this group of hackers selected its members and what features mentioned by recruits were particularly valued. We then used this dataset to perform targeted qualitative analysis concerning some individuals and products that appeared to be of particular interest. In the following section, we describe the main arguments used by applicants to gain acceptance into this community, as well as the types of responses generated by different types of skills and experience.

[INSERT FIGURE 3 ABOUT HERE]

What hackers talk about when they talk about hacking: Presentational strategies

The detailed coding of introductions, which were very diverse in length and format although they generally followed the script outlined by Sp3cial1st in Figure 2, followed an inductive process adapted from previous work on reputation and trustworthiness in online cybercrime forums (Dupont et al., 2016). In their analysis of 25,000 reputation ratings, Dupont et al. (2016: 14) identify five categories of feedback that justify positive of negative ratings: the level of satisfaction with a past business relationship, the type of general contribution to the community, a specific behavior directed at the feedback provider, the quality of technical skills, and sarcasm. A first high-level reading of the introductions led us to remove the "sarcasm" category, irrelevant in that context, and to make minor adjustments the four other categories to classify the signals of trustworthiness sent by candidates to the community: who they knew in the forum (sponsors), mentions of their track record on other forums or with particular hacking teams (experience), a description of their hacking abilities, in terms of both uniqueness and relevance (technical skills), and the role they expected to play in the market (business interests). When the information was available, we also recorded the types of malware and services they were selling. We used the same categories to classify responses by established members, which allowed us to compare what applicants thought the community valued most with what actually attracted attention or scorn from active members. Table 1 provides the descriptive statistics for the distribution of introductions across the four categories described above. In the next paragraphs, we provide additional details on each of those four dimensions, from both candidates and established members' perspectives. To illustrate how each category of trustworthiness argument was used by applicants and what type of responses it elicited, we selected a number of quotes that we believe are most representative of our sample, even if such claims are always subjective when qualitative data is analyzed. Before we go any further, we should note that, among the 277 applications to join the forum for which we know the outcome with certainty, 94.5% were successful, which was counterintuitive considering the claims to exclusivity made by Darkode administrators.

[INSERT TABLE 1 ABOUT HERE]

Sponsors: 90.7% of introductions to the forum mention the name of the sponsor who provided the initial invitation, reflecting the importance of personal ties in admission to this group. Very few of the candidates provide more detailed contextual information that reveals the nature of these linkages, but a small group of forum administrators appeared to be responsible for a large share of sponsorships. The 286 introductions that acknowledge invitations mention 119 Darkode members, with an average of 2.4 invitations converted into applications per referrer (median: 1, range: 1-46). However, the four most influential recruiters (Sp3cial1st, G0dlike, Mafi, and Fubar), who were also forum administrators, accounted for 38% of invitations. Without their constant efforts to promote the forum and scout potential new members, the growth of this network through regular members' referrals would not have been sufficient to sustain the community's expansion. For example, high profile members such as Gribodemon, Paunch, or Bx1 brought in only a couple of new members each, focusing their energies on marketing their own successful products rather than on growing the community of purchasers. Although trustworthiness was the most frequently cited argument for admitting or refusing membership, very few members assessing new candidates commented on the identity or track record of their sponsor (a mere 19.5%), seeming to take the transferability of trustworthiness for granted. The following quote from a Level 1 member perfectly summarizes this vicarious form of trust: " "I was invited here by mafi." u got me when I saw this. this guy sounds cool".

Technical skills: The second strategy to gain acceptance was to demonstrate one's potential contribution, with particular emphasis on the unique and relevant technical skills that differentiate "script kiddies" from the more advanced programmers who design and build the malware used by the former. 69.5% of applicants listed their technical skills, with a majority claiming to have mastered generic coding techniques and common programming languages such as C/C++, Javascript, Python, or Perl (60%), while a smaller group advertised more specialized skills such as reverse engineering (12%), obfuscation and encryption techniques (6%), sql injection (5%), or traffic theft (2%). Interestingly, only seven candidates (2%) claimed they had the expertise to find 0-day exploits, the highly prized undisclosed vulnerabilities against which no computer system is protected (Bilge & Dumitras, 2012). Technical skills arguments elicited only 15.1% of comments, usually to confirm that a candidate had indeed programmed certain products to the satisfaction of existing members, sometimes noting the outstanding quality of the code delivered.

Experience: Before they applied, many candidates had been active on other cybercrime forums and used these types of experience to gain admission to Darkode, especially when they had worked their way up and held verified status or administrative roles in other forums. Some candidates who had developed and marketed popular malware also made sure to mention these in their introduction. Experience accumulated on other forums or selling particular products was mentioned in 49.7% of introductions and triggered the largest share of responses (48.5%), often confirming that a particular member using the same alias had been active on said forum and had behaved reliably. The experience factor was the content category that resonated most with existing members, who seemed to be reassured by the fact that a candidate's track record could be verified independently.

Business: 49.4% of candidates included in their introduction the types of transactions they expected to conduct on Darkode, either as sellers or buyers of products, services, or stolen data.

Buyers significantly outnumbered sellers, with 31% of applicants who emphasized business credentials identifying themselves as sellers and 69% as buyers. Products listed as available included botnets, malware tools, databases of stolen personal information or accounts, proxy services, encryption solutions to evade detection, as well Internet traffic that could lead to criminal exploitation. Most business statements mentioned specific products that could be obtained from them or that they were seeking to buy. For example, Exmanoize claimed in his introduction to be the seller and author of the Eleonore exploit kit, which became popular among hackers in 2009 (Chen & Li, 2015). Such statements would seem to be beneficial because a candidate who had established a recognized brand through a popular product could increase his chances of being accepted into the community through public support from past customers. Less than one fifth of comments (18%) addressed these business credentials, often by confirming that a member had smoothly conducted transactions with an applicant and that the products and services were of the advertised quality. The purchasing power of potential new members was also a highly rated feature.

Hence, while candidates tried to earn the trust of their peers by associating themselves with established participants, showcasing a broad palette of attractive technical skills, and leveraging reputational capital accumulated on other underground forums, existing members seemed most responsive to the Fresh Fish's previous experience and their business potential. But in the end, these four presentational strategies did not seem to enable very discriminatory selection patterns among voting members, considering that only 7% of comments in the introductions we reviewed expressed distrust. As a result, a vast majority of applicants were granted access to Darkode and allowed to interact with high profile hackers eager to expand their customer base.

The business challenges faced by prolific sellers

Once admitted to the forum, Level 0 members had the opportunity to buy, sell, and trade a broad range of cybercrime products and services and to comment on their quality and affordability. They were also free to participate in technical problem-solving conversations or in off-topic discussions about a very broad range of subjects, from high profile arrests to pornography, psychoactive substances, religion (when Ramadan started for example), or even Area 51, the secret military base in the Nevada desert. As well, administrators organized hacking challenges that allowed members to display their technical skills. In this section, we discuss two areas closely connected to the day-to-day operations of this illicit market and show how, despite the selection procedure described above, which looked exacting only in appearance, many interactions between buyers and sellers were dysfunctional, undermining the performance of the market. We start by analyzing the trades conducted by Bx1 and compare the outcome of one of his largest transactions with the financial losses attributed to him by the Justice Department. We selected this particular member for three main reasons: he was at the time the principal marketer for one of the most effective banking malware ever designed (Kirk, 2011), maintained a very active profile on the forum, and was subsequently arrested, prosecuted and sentenced by the U.S. government. This produced a rich trail of publicly available legal documents that made the comparison interesting between the interactions he had on Darkode with co-offenders and how his case was presented to public opinion. We then shift our focus from the traders operating in this market to the products being exchanged in

order to highlight the specific challenges associated with the sale of hacking tools to malicious hackers who often do not hesitate to leak them, thereby compromising the business opportunities of their designers. To illustrate this point, we use the example of Crimepack, a piece of malware developed and marketed by one of Darkode's administrators that was leaked shortly after the release of a technical update. This case study shows how even one of the forum's most powerful members could not prevent others from undermining his business.

What criminal achievement looks like from the U.S. Government and Darkode's perspectives

Bx1 was one of the most active and successful members of the Darkode forum, where he sold a popular banking trojan called SpyEye that he had helped develop. SpyEye stole the online banking credentials of its victims and hijacked web sessions so that its operators could easily and stealthily take over their victims' accounts. Although such numbers are always highly controversial, the U.S. Justice Department estimated that SpyEye had infected more than 50 million computers—targeting 253 discrete financial institutions – and had caused close to a billion dollars in financial harm. Known as the smiling hacker for his relaxed attitude in pictures taken following his arrest by the Thai police on 5 January 2013, while he was in transit from Malaysia to Algeria, Bx1's real identity was revealed to be Hamza Bendelladj, a 24-year-old Algerian national (Krebs, 2013). He was extradited to the U.S. in May of the same year, pleaded guilty to all 23 counts of his indictment, and was sentenced to 15 years in jail in April 2016 (U.S. Attorney's Office, 2016). Even if he was not SpyEye's main designer, he played an instrumental role in developing customized modules and marketing the malware. He also used SpyEye himself to collect large quantities of stolen banking credentials, which he also sold on Darkode.

The sentencing memorandum filed by the U.S. Attorney provided a detailed account of Bendelladj's dealings and requested an exemplary sentence based on incurred financial losses estimated to have reached $100 million. The Department of Justice (DOJ) arrived at such an impressive number after having revealed that Bx1's seized laptops contained more than 200,000 full credit card records (including numbers, owners' name and address, and card CVV – the three digit security number found at the back of these cards) and that he had "cashed out millions of dollars stolen from bank accounts across the world" (Horn et al., 2016). Although the sentencing memorandum noted that credit card issuers and banks had documented only about $3.25 million dollars in attempted fraud and $878,000 in effective losses, the U.S. Attorney's Office still applied sentencing guidelines that valued losses at a minimum of $500 per card, producing an impressive global amount that would capture any judge's attention. A closer look at the discussions initiated by Bx1 and his peers' responses illustrate clearly how such calculations might have distorted the profitability of his business and been misleading.

On 3 December 2011, Bx1 started a thread on the forum advertising the sale of a freshly hacked "shopadmin database" containing more than 140,000 orders. A "shopadmin" is the common technical designation of a web interface used by online merchants to manage their store, keep track of customers and their orders, and manage payments and deliveries. Most orders in this database were shipped to the U.S. and Canada, so Bx1 was able to offer highly valued credit card numbers from those two countries, including their expiration date, CVV, an associated billing and shipping address, and the email and password used by customers to register an account on the compromised website from which the data had been stolen.

Asked by a Level 2 member what the starting bid for this database was, Bx1 suggested opening the bidding at $20,000. This is far less than what the DOJ formula presented above suggests as the projected profits that can be generated from these types of frauds. Unfortunately for Bx1, the first offer made by a forum member named Donchicho seriously dampened his initial hopes, offering $300 for the whole database. Bx1 replied that: "if I sell 0.5$ each cc [credit card] I get 50k guaranteed." Even if we ignore Bx1's shaky math, we are still four orders of magnitude below the DOJ's calculations for the average financial loss associated with a stolen credit card. Swayed by Bx1's plea, MrGold, another Level 2 member, made a $2,000 bid, which was promptly rejected on different grounds: "I tested 6 out of 160k Diffe [different] Dates. Means from 2008-2011. And all approved. I can test for interested buyer and I show them VIA Team Viewer [a software allowing desktop sharing]." But this argument, intended to highlight the quality and reliability of the stolen data, was in turn disputed by Sven, a Level 2 member, who explained: "You can test 100 and 100 out of 100 work. When you use about 6-8k of the total 160k, all base [anti-fraud banking databases] will go nuts and you get ~ 20% approvals." Perhaps sensing Bx1's weakening negotiating position, MrGold made a final $3,000 offer. It may very well be that another hacker eventually concluded a more generous deal with Bx1 through private channels (a common occurrence), but the exchanges between seller and potential buyers on this thread still give a sense of the wildly fluctuating pricing mechanisms at work, which probably reflect the difficulty of cashing in on these types of stolen databases.

The challenge faced by Bx1 was not only to obtain the price he expected for the stolen data but also to maintain the satisfaction of his clients and, by extension, his reputation as a reliable hacker to do business with. In an enlightening exchange started on 27 May 2011, Bx1 advertised a "spreader," a piece of software that automates the dissemination of malicious code needed to enroll vulnerable machines into a botnet through popular online services such as Facebook, Twitter, Gmail, or Hotmail. After a few flattering comments from members noting the effectiveness of the product for sale, the conversation took a more personal turn when Solotech, a Level 1 member, complained that he had not received the most recent technical update for this spreader, to which he felt he was entitled. Additionally, he voiced his displeasure about Bx1's unresponsiveness. Less than twelve hours later, Bx1's answer acknowledged that he had indeed not sent the update but that this decision had been motivated by Solotech's veiled threats to publicly release the code of the spreader, which would have threatened Bx1's business. This spurred Gonzo, an administrator who had positively commented on the malware for spreading "like Aids," to come to Solotech's defense: "Bro, I know Solotech for a while now. He is a standup guy, maybe he was saying that out of anger." Another administrator, Sp3cial1st, took a more confrontational approach toward Bx1: "Been waiting approx 1 week for a reply from you bx1! Messaged you with some questions about how it works and so forth but no reply." By 25 June 2011, a third administrator, Fubar, had also publicly taken sides with Solotech, trying to justify his erratic behavior by the fact that Solotech had purchased the original version of this malware from another hacker (Jam3s) with exclusive use rights for $10,000 and was irritated to find out Bx1 had taken over this project and he had to pay an extra $1,500 for the newer and more stable version. Meanwhile, potential buyers' queries were drowned out in the intensifying exchanges trying to assess the validity of Bx1 and Solotech's arguments. In other words, what started as a routine marketing post morphed into a public discussion debating the legitimacy of Bx1's business practices and questioning his commitment

to customer service. A post from Tux reflected that frustration:

> Will you be back by the end of this year, cause I remember when similar members said going to vacation… and they disappeared for like 4-7 months causing me a lot of pain in the ass while time to complete business wouldn't take more then 30 minutes to max couple of hours. In that time they were relaxing, swimming or getting high I lost allot of money I could earn, basically I had opportunity cost cause of their vacation…

Bx1's position had shifted to a defensive posture in which he was compelled to justify his business practices and clarify his dispute with Solotech in order to maintain his reputation. A lengthy post dated 2 July 2011, summarizes this damage control operation:

> I asked about u [Solotech] and 1/10 says u're good rest all says No.
> And I still have your conversation when you said You gonna make it public and I don't take shit of this.
> …You can post me on scammer [a list of untrustworthy traders] or anywhere you like, everyone knows me here I gave all what they purchase and also I was giving them gifts in vcc's sales [virtual credit cards] and if I didn't that or scam someone he post here or post me on scammer, and if any coder is on my place he will do same like me. Just lets see people what they say.
> Guys just say,
> Do you give someone update if he says he gonna make it public?
> Yes or No

No honor among thieves: leaks and the dilemmas of protecting cybercriminal intellectual property

This final question is not a rhetorical one, as the leaking of proprietary hacking software is a common occurrence that undermines the profits of malware marketers. Mafi for example, the forum administrator indicted in the July 2015 takedown, complained bitterly to the community on 26 September 2010[1] about the leak of his own Crimepack exploit kit on the Contagio Malware Dump blog:[2]

> Crimepack leak?
> What the fuck is the problem with you guys?
> The only people that have version 3.1.3 is people on this board and how come a security researcher gets a hold of a copy of it?
> You guys better start acting as fucking professionals sometime all the leaks of Crimepack so far has been thanks to people on this forum and we are supposed to hold a higher fucking standard.
> I suppose in the future I will only be able to sell & give updates to very limited people and rule out the rest.

The conversation then proceeded to try to identify the source of the leak, with the possibility

being raised that a mole had infiltrated the group. A more disturbing explanation was the possibility that one of the forum's members had been compromised, somehow discrediting the mythology of Darkode as an exclusive community of elite hackers. Mafi himself was not exempt from questions about his operational security skills, one member (The Rogue) asking: "Why didn't you put various tags in the code and such? Like rearrange block list or something. Then when they [security researchers] post info, you can tell who leaked it?" Sp3cial1st also made his displeasure known in no uncertain terms: "I literally just got around to finally fucking uploading and installing the non domain locked crimepack and now it is basically useless. Goddamit someone needs to be fucking murdered!" To reassure forum members, Mafi stressed that the obfuscation technique he used should prevent security researchers from learning too much about the malware's functions and that it therefore remained a useful hacking tool worth purchasing. And indeed, this was subsequently confirmed by academic researchers who noted that Crimepack had been encoded using a very effective commercial protection software called IonCube (Kotov and Massacci, 2013). However, as a result of the uncertainty created about the source of the leak and the need to prevent further exposure, Mafi limited the distribution of updates to a few trusted customers, thereby restricting new sales opportunities and profits. Furthermore, numerous posts discussed who could have betrayed Mafi's trust, how he could be identified (someone suggested that the list of Crimepack buyers should be disclosed and then there would be a vote on potential suspects), what his motivations were (greed or stupidity), whether federal agents were involved in the forum's infiltration, and how the potential suspect should be dealt with once identified (some called for "good old fashion russian dismemberment," while others felt more forgiving, recommending "rape him a little").

Even if one should not interpret the contents of these posts too literally, the sense of drama and paranoia created by this kind of business transgressions and their aftermath proved detrimental to the effective functioning of this market. The situation became so problematic that a "no leaking" policy was announced in March 2011 by Godlike, one of the forum's administrators:

> Leaking will not be tolerated anymore. Please respect members work.
> When you leak, you make authors think again before releasing their tools.
> If you decide to leak you will be banned without warning, this applies to tools that will effect members of the forum.

Predictably, in a number of posts that grew exponentially, some members wondered how this new policy would work as the complexity of designing, implementaing and enforcing an effective anti-leaking policy became obvious. The questions that were debated among members included the following, with administrators' answers in parenthesis: Would the ban be comprehensive or limited to activities on Darkode while tolerating leaking on other forums? (No clear answer.) Would the policy still be enforceable once leaked malware had been widely distributed by others? (Yes, in order to avoid publicly disrespecting members.) Should malware programmed by members of beginners' forums be exempted from the no leaking policy? (Yes.) If yes, what would happen if their developers were invited to join Darkode at a later date? (The leak would then be removed from the forum.) These questions highlighted the inherent tension between hackers' natural propensity to probe, reverse engineer, and disclose software code, on

one hand, and the need for any market, including an illicit one with restricted access, to adopt and enforce regulations protecting the intellectual property rights of sellers, on the other. The frustration expressed by Darkode's administrators reflected the chaotic nature of exchanges in this particular community.

Conclusion

This paper's primary contribution is to analyze the outcomes of an elite hacking forum's selection process, and to develop a better understanding of how trust is established in online markets where participants are vetted by their peers. This is the first time, to the best of our knowledge, that data about such an exclusive and closed group of cybercriminals is explored in depth. However, we did not anticipate that we would uncover a situation where the vast majority of candidates were let in for profit purposes, in contradiction with the disciplined and security-minded image projected by the forum administrators. Despite the detailed admission procedures designed by administrators, the forum seems to have faced the same trust and reliability problems as those documented in previous research on public cybercrime channels and forums (Herley and Florêncio, 2010; Holt and Lampke, 2010; Yip et al., 2013b; Dupont et al., 2016). Based on the evidence derived from a partial analysis of this dataset, we find a high acceptance rate (94.5%) for new members that contradicts the narrative of an elite forum accessible only to highly skilled hackers. Provided that a candidate was able to obtain an invitation—and administrators made sure that many were extended to members of less-exclusive forums (MalwareTech, 2014)—the chances of gaining entry were overwhelmingly positive. This unexpectedly high acceptance rate was sustained to a large extent by the belief that a proven track record on another hacking forum and a willingness to conduct business on Darkode were more desirable features than the ability to demonstrate advanced technical skills, a demand that would have produced more discriminatory outcomes. Analysis of introductions confirmed that a majority of applicants claimed to have mastered only very common programming techniques and that more complex skills such as obfuscation, cryptography, and sql injection were in much shorter supply. As one of its co-founders candidly acknowledged, such a configuration was almost inevitable, given a core group of talented hackers designing powerful malware who needed to find and cultivate buyers for their products (Placek, 2016). In other words, when the administrators had to choose between a close-knit community of technical experts sharing common values and a more open market catering to cybercrime entrepreneurs, they put profits before trust, which possibly led to their demise.

As a result, and despite what may arguably have been the most elaborate attempts yet by an online illicit market to shut out rippers and eradicate deceptive practices, trust remained elusive and interactions were often fraught with suspicion and accusations. This sense of paranoia was made more acute by evidence that the forum had been repeatedly infiltrated by law enforcement investigators, security researchers, and the occasional investigative journalist, putting a lot of pressure on members. Many threads that began as technical and business discussions escalated rapidly into smear campaigns that mobilized considerable amounts of energy and became major distractions for a community that had been designed initially to improve the quality of collaboration among proficient hackers. So, we did not progress as expected in establishing what features and traits enhance the reputation and trustworthiness of new entrants in online illicit

markets, but our results suggest that frequent expressions of distrust and defiance are found across the whole spectrum of hacker communities, from beginners' forums (Dupont et al., 2016) to a high-end market such as Darkode. This insight is a new contribution to the literature that will need to be confronted with further empirical evidence in order to test its generalizability. For example, can innovative technical solutions such as the automated cryptographic, reputational and escrow mechanisms found on cryptomarkets overcome this trust deficit and usher a new transformative era of cybercrime effectiveness (Aldridge and Décary-Hétu, 2014)? Alternatively, do hybrid cybercrime networks that blend offline and online social ties prove more resilient than their purely online counterparts as far as trust is concerned (Leukfeldt et al., 2016b)?

For a traditional online forum such as Darkode, one of the consequences of such high levels of distrust are the difficulties and resistance that even one of its most successful members, such as Bx1, encountered when he tried to sell his products, services, or stolen data. The estimated revenue from the big volume sale we analyze in this paper proved to be very different from the financial loss estimated by the Department of Justice in Bx1's sentencing memorandum—different by several orders of magnitude. While we acknowledge that our analysis does not include the costs of the harm caused by the identity fraud that this sale made possible, and that we were not able to perform a complete analysis of all the transactions conducted by Bx1 on this forum and in other online illicit markets, the discrepancy remains significant and deserves to be investigated further in future research, particularly given the lengthy jail sentences that have been imposed in similar cases. We have not found in the literature any other contribution attempting a comparison between the financial harm caused by online offenders and the claimed harm publicized by law enforcement investigators and prosecutors following high profile convictions, and we therefore believe that researchers should continue their work on methodologies that produce more robust numbers.

The qualitative analysis of several threads discussing leaks of malware and the best ways to prevent them highlights how challenging it was for malicious developers to protect their intellectual property and to maintain sustainable revenue streams. While they struggled to keep their fickle customers happy, disloyal competitors or cybercrime wannabes did not hesitate to crack code they had written and share it for free or at bargain prices. In future studies, we plan to dig much deeper into the data to understand how disputes and distrust arose, how the former were adjudicated to limit the latter, and what was the impact on forum's operations. The financial harm caused by Darkode members was certainly not trivial, but results taken from a small sample of high profile hackers show that their criminal experiences and achievements diverged significantly from the myth of the lone super-hacker (Ohm, 2008) that is often generated by security firms and law enforcement agencies, and obligingly amplified by the mass media. Like their offline criminal entrepreneur counterparts, their success seemed to depend as much on their ability to prevent or overcome the malfeasance, mistakes, or failures (von Lampe and Johansen, 2004; Tilly, 2005) that invariably punctuated their dealings with other hackers as on their technical expertise.

Notes

[1] Although the post is dated 26 September 2010, the first mention of a Crimepack leak in the media and on specialized security blogs appeared only in May 2011. This discrepancy may be attributable to a delay in publicizing the leak or to a timestamping error.
[2] http://contagiodump.blogspot.ca

References

Ablon, L., Libicki, M., & Golay, A. (2014). *Markets for cybercrime tools and stolen data: Hacker's bazaar*. Santa Monica, CA: RAND Corporation.

Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013). Honor among thieves: A common's analysis of cybercrime economics. *2013 eCrime Researchers Summit*, San Francisco, 17-18 September 2013. Retrieved from http://www1.icsi.berkeley.edu/~sadia/papers/ecrime13.pdf.

Akerlof, G. (1970). The market for "lemons": Quality incertainty and the market mechanism. *The Quarterly Journal of Economics, 84*, 488-500.

Aldridge, J., & Décary-Hétu, D. (2014, May 13). Not an 'Ebay for drugs': The cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. Retrieved from https://ssrn.com/abstract=2436643.

Allodi, L., Corradin, M., & Massaci, F. (2016). Then and now: On the maturity of the cybercrime markets – The lessons that black-hat marketeers learned. *IEEE Transactions on Emerging Topics in Computing, 4*, 35-46.

BBC (2013, December 24). *Mariposa botnet 'mastermind' jailed in Slovenia*. Retrieved from http://www.bbc.com/news/technology-25506016

Best, J., & Luckenbill, D. (1994). *Organizing deviance*. Upper Saddle River, NJ: Prentice Hall.

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 833-844). New York, NY: ACM.

Chen, J., & Li, B. (2015). *Evolution of exploit kits: Exploring past trends and current improvements*. Irving, TX: Trend Micro.

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*, 160-175.

Décary-Hétu, D., & Laferrière, D. (2015). Discrediting vendors in online criminal markets. In A. Malm & G. Bichler (Eds.), *Disrupting criminal networks: Network analysis in crime prevention* (pp. 129-152). Boulder, CO: Lynne Rienner.

Décary-Hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal, 29*, 442-460.

Décary-Hétu, D., & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, doi:10.1007/s10611-016-9644-4.

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*, 129-151.

Europol (2015, July 15). *Cybercriminal Darkode forum taken down through global action*. Retrieved from https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action

FBI (2010, July 28). *FBI, Slovenian and Spanish police arrest Mariposa botnet creator, operators*. Retrieved from https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-slovenian-and-spanish-police-arrest-mariposa-botnet-creator-operators

FBI (2015, July 15). *Major computer hacking forum dismantled*. Retrieved from https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/major-computer-hacking-forum-dismantled

Felson, M. (2003). The process of co-offending. In M. Smith & D. Cornish (Eds.), *Theory for practice in situational crime prevention* (pp. 149-168). Monsey, NY: Criminal Justice Press.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An inquiry into the nature and cause of the wealth of Internet miscreants. In *Proceedings of the 14th ACM Conference on Computer and Communications Security* (pp. 375-388). New York, NY: ACM.

Glenny, M. (2011). *DarkMarket: Cyberthieves, cybercops and you*. New York, NY: Alfred A. Knopf.

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* (pp. 33-53). New York, NY: Springer.

Holt, T., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies: A Critical Journal of Crime, Law and Society, 23*, 33-50.

Holt, T. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, *14*, 155-174.

Holt, T., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime, 16*, 81-103.

Holt, T. (2016). Identifying gaps in the research literature on illicit markets on-line. *Global Crime,* doi: 10.1080/17440572.2016.1235821.

Holt, T., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior, 37*, 353-367.

Horn, J., Ghali, K., & Grimberg, S. (2016). *United States of America v. Hamza Bendelladj (A. K. A. "Bx1") Criminal Action No. 1:11-CR-557-AT-2 Sentencing Memorandum*. Retrieved from http://krebsonsecurity.com/wp-content/uploads/2016/04/bx1-gribboSM.pdf

Hrodey, M. (2015, October 12). Dark Side. *Milwaukee Magazine*. Retrieved from https://www.milwaukeemag.com/2015/10/12/dark-side-darkode-fbi/

Hutchings, A., & Holt, T. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*, 596-614.

Hutchings, A., & Holt, T. (2016). The online stolen data market: disruption and intervention approaches. *Global Crime*, doi: 10.1080/17440572.2016.1197123.

Kharouni, L. (2015, December 1). Darkode reloaded – New forum gets "F" grade. *Day Before Zero Blog*. Retrieved from https://www.damballa.com/darkode-reloaded-new-forum/

Kirk, J. (2011, July 26). SpyEye Trojan defeating online banking defenses. *Computerworld*. Retrieved from http://www.computerworld.com/article/2509482/security0/spyeye-trojan-defeating-online-banking-defenses.html.

Koster, M. (1996). *A method for web robots control*. Retrieved from http://www.robotstxt.org/norobots-rfc.txt

Kotov, V., & Massacci, F. (2013). Anatomy of exploit kits: Preliminary analysis of exploit kits as software artefacts. In J. Jürjens, B. Livshits & R. Scandariato (Eds.), *Engineering secure software systems* (pp. 181-196). Berlin: Springer Berlin Heidelberg.

Krebs, B. (2011, October 17). Software pirate cracks cybercriminal wares. *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2011/10/software-pirate-cracks-cybercriminal-wares/

Krebs, B. (2013a, April 2). Fool me once… *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2013/04/fool-me-once/

Krebs, B. (2013b, May 3). Alleged SpyEye seller 'Bx1' extradited to U.S. *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2013/05/alleged-spyeye-seller-bx1-extradited-to-u-s/

Krebs, B. (2014). *Spam nation: The inside story of organized cybercrime – from global epidemic to your front door*. Naperville, IL: Sourcebooks.

Krebs, B. (2015). *The Darkode cybercrime forum, up close*. Retrieved from https://krebsonsecurity.com/2015/07/the-darkode-cybercrime-forum-up-close/

Leukfeldt, E. R., Kleemans, E., & Stol, W. (2016a). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology,* doi: 10.1093/bjc/azw009.

Leukfeldt, E. R., Kleemans, E., & Stol,W. (2016b). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, *67*, 39-53.

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*, 31-41.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*, 71-94.

Macdonald, M., & Frank, R. (2016). The network structure of malware development, deployment and distribution. *Global Crime,* doi: 10.1080/17440572.2016.1227707.

MalwareTech (2014). *Darkode – Ode to Lizard Squad (the rise and fall of a private community)*. Retrieved from https://www.malwaretech.com/2014/12/darkode-ode-to-lizardsquad-rise-and.html

McCoy, D., Pitsillidis, A., Jordan, G., Weaver, N., Kreibich, C., Krebs, B., Voelker, G., Savage, S., & Levchenko, K. (2012). PharmaLeaks: Understanding the business of online pharmaceutical affiliate programs. *21st USENIX Security Symposium,* Bellevue, WA, 8-10 August 2012. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final204.pdf.

Monsma, E., Buskens, V., Soudijn, M., & Nieuwbeerta, P. (2013). Partners in cybercrime. In D. F. Hsu & D. Marinucci (Eds.), *Advances in cyber security: Technology, operations and experiences* (pp. 146-172). Bronx, NY: Fordham University Press.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. (2011). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, New York, NY: ACM.

Office for National Statistics (2016). *Crime in England and Wales: Year ending June 2016*. London: ONS.

Ohm, P. (2008). The myth of the superuser: Fear, risk, and harm online. *UC Davis Law Review, 41*, 1327-1402.

Pauli, D. (2013, September 12). The rise of the white hat vigilante. *IT News*. Retrieved from http://www.itnews.com.au/news/the-rise-of-the-white-hat-vigilante-356543/page0

Placek, M. (2016). Daniel Placek on Darkode. *Lawfare Podcast*, episode 157. Retrieved from https://www.lawfareblog.com/lawfare-podcast-daniel-placek-darkode

Poulsen, K. (2011). *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. New York, NY: Crown Publishers.

Saldaña, J. (2009). *The coding manual for qualitative researchers*. London: SAGE Publications.

Soudijn, M., & Zegers, B. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*, 111-129.

Tilly, C. (2005). *Trust and rule*. Cambridge: Cambridge University Press.

Turton, W. (2015, August 9). The year of the Lizard Squad. *The Kernel*. Retrieved from http://kernelmag.dailydot.com/issue-sections/features-issue-sections/13941/who-is-lizard-squad-history/

U. S. Attorney's Office (2016, April 20). *Two major international hackers who developed the "SpyEye" malware get over 24 years combined in federal prison*. Retrieved from https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined

Von Lampe, K., & Johansen, P. (2004). Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime, 6*, 159-184.

Xylitol (2013, April 1). *Darkode leak*. Retrieved from http://www.xylibox.com/2013/04/darkode-leak.html

Yip, M., Shadbolt, M., & Webber, C. (2012). Structural analysis of online criminal social networks. *International Conference on Intelligence and Security Informatics*, Arlington, 11-14 June 2012. Retrieved from http://eprints.soton.ac.uk/337076/1/yip_isi2012_final.pdf.

Yip, M., Shadbolt, N., & Webber, C. (2013a). Why forums? An empirical analysis into the facilitating factors of carding forums. *ACM Web Science 2013*, Paris, 2-4 May 2013. Retrieved from http://eprints.soton.ac.uk/349819/1/yip_websci13_final.pdf.

Yip, M., Webber, C., & Shadbolt, N. (2013b). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society, 23*, 516-539.

Zetter, K. (2015, July 15). Dozens nabbed in takedown of cybercrime forum Darkode. *Wired*. Retrieved from https://www.wired.com/2015/07/dozens-nabbed-takedown-cybercrime-forum-darkode/

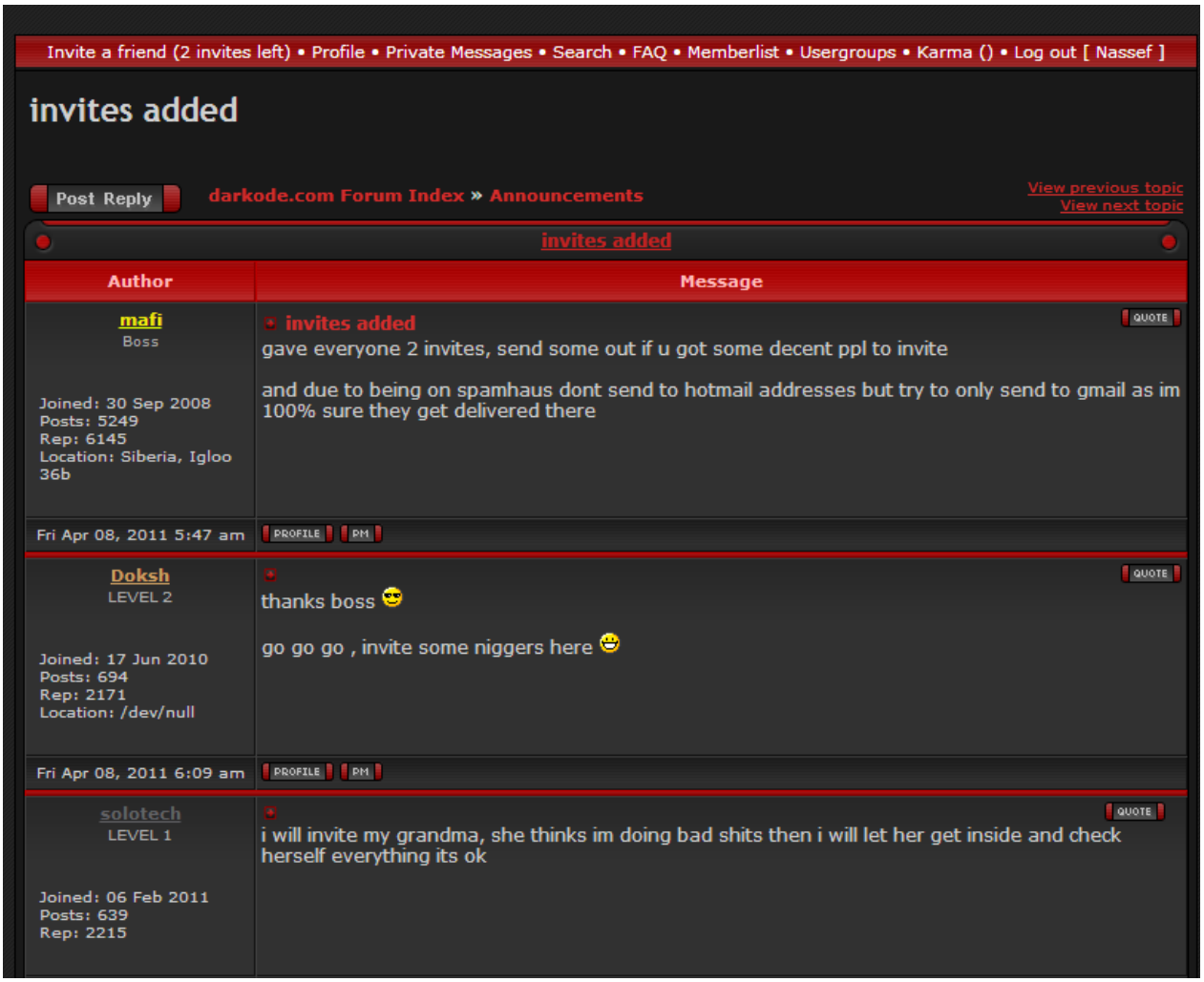
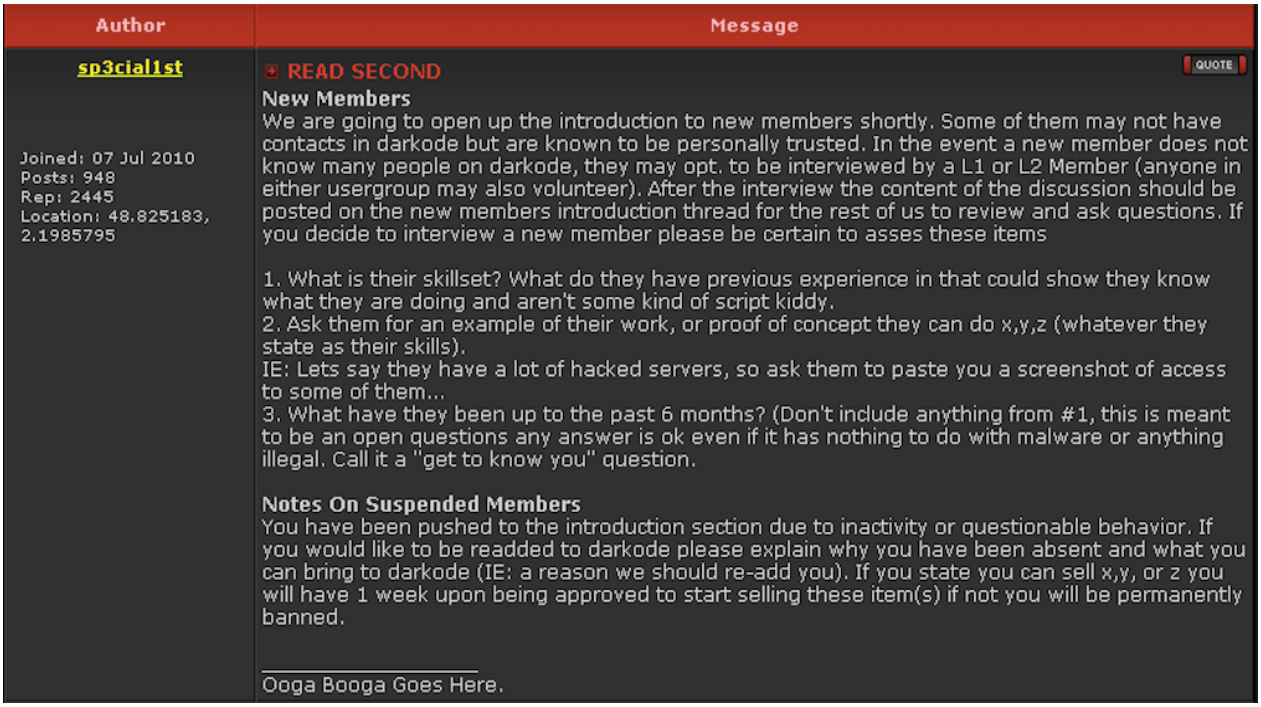


Figure 1. Darkode screenshot.



Author	Message
sp3cial1st Joined: 07 Jul 2010 Posts: 948 Rep: 2445 Location: 48.825183, 2.1985795	READ SECOND QUOTE **New Members** We are going to open up the introduction to new members shortly. Some of them may not have contacts in darkode but are known to be personally trusted. In the event a new member does not know many people on darkode, they may opt. to be interviewed by a L1 or L2 Member (anyone in either usergroup may also volunteer). After the interview the content of the discussion should be posted on the new members introduction thread for the rest of us to review and ask questions. If you decide to interview a new member please be certain to asses these items 1. What is their skillset? What do they have previous experience in that could show they know what they are doing and aren't some kind of script kiddy. 2. Ask them for an example of their work, or proof of concept they can do x,y,z (whatever they state as their skills). IE: Lets say they have a lot of hacked servers, so ask them to paste you a screenshot of access to some of them... 3. What have they been up to the past 6 months? (Don't include anything from #1, this is meant to be an open questions any answer is ok even if it has nothing to do with malware or anything illegal. Call it a "get to know you" question. **Notes On Suspended Members** You have been pushed to the introduction section due to inactivity or questionable behavior. If you would like to be readded to darkode please explain why you have been absent and what you can bring to darkode (IE: a reason we should re-add you). If you state you can sell x,y, or z you will have 1 week upon being approved to start selling these item(s) if not you will be permanently banned. _____ Ooga Booga Goes Here.

Figure 2. Introduction guidelines screenshot.

Figure 3. Introduction screenshot.

Table 1. Frequency distribution for four categories of arguments used by candidates in their introduction and by members in their assessment (N=344)

Categories	***Introductions***		***Answers from existing members***	
	%	**N**	**%**	**N**
Sponsor	90.7	312	19.5	67
Technical skills	69.5	239	15.1	52
Experience	49.7	171	48.5	167
Business	49.4	170	18.0	62

Note: as each introduction contained signals of trustworthiness belonging to different categories, the sum is greater than 100%.