Skills and trust: a tour inside the hard drives of computer hackers

Benoit Dupont[1]

School of Criminology, University of Montreal

Abstract: Stories of the exploits of computer hackers who have broken into supposedly secure government and corporate information systems appear almost daily on the front pages of newspapers and technology websites, yet we know very little about the individuals behind these headlines. Most media accounts and academic studies on hackers suffer from a number of biases that this research attempts to overcome. A case study based on the seized communication logs of ten confirmed co-offenders is used to expand our knowledge of the social norms and practices that govern interactions between malicious hackers. After presenting the data and how the material became available to the author, the remaining sections focus on the two variables that define this criminal network's performance: skills and trust. The skills under consideration are the three different sets of cognitive and practical abilities that malicious hackers need in order to succeed financially. Monetization and social skills, in addition to technical skills, play key roles in profit-oriented malicious hacking and explain why earning a decent living in the computer underground remains a laborious endeavour, even for advanced hackers. Trust, which facilitates the diffusion of technical, monetization, and social skills and fosters collaboration, was found to be much lower in this network than is generally assumed in the literature. The need for monetization and social skills as well as the lack of trust between members may partly explain why hacker networks are so ephemeral and vulnerable to law enforcement disruption.

Keywords: Malicious hackers, botnet, social network analysis, trust, technical skills, social skills, monetization skills

[1] The author would like to acknowledge the invaluable help of the Sûreté du Québec, without which this research would not have been possible. Errors in the interpretation of the data remain his own.

Introduction

Stories of the exploits of computer hackers who have broken into supposedly secure government and corporate information systems appear almost daily on the front pages of newspapers and technology websites, yet we know very little about the individuals behind these headlines. They are often caricatured as socially inept (Denning, cited in Leeson and Coyne 2005: 518) but intellectually gifted teenagers who unleash a technical apocalypse on their helpless victims from the solitary confines of their parents' basements, a representation fuelled to a large extent by Hollywood movies.[2] This stereotype is helped by the very limited number of arrests made by the police, and the even smaller number of cases that go to trial, as most of the accused plead guilty in order to negotiate a favourable arrangement with prosecutors. The resulting lack of real-life accounts describing malicious computer hackers and how they operate means that policy-makers and criminal justice practitioners as well as members of the public rely on fictional depictions or self-aggrandizing autobiographies (Mitnick and Simon 2011, Calce and Silverman 2008) to make sense of this new class of offenders.

Academic publications are unlikely to alter this stereotype any time soon. Not only are they disproportionally few compared to those in the general media but most of the πacademic literature on the subject originates from computer science researchers who focus on the technical or economic aspects of hacking and demonstrate little interest in its social dimension. A few psychologists (Schell et al. 2002; Rogers 2006; Young et al. 2007), sociologists (Jordan and Taylor 2008; Turgeman-Goldschmidt 2009), anthropologists (Coleman and Golub 2008), and criminologists (Hollinger 1991; Yar

[2] Such as such as *WarGames* (1983), *Sneakers* (1992), *Hackers* (1995), *The Net* (1995), *Swordfish* (2001), *Live Free or Die Hard* (2007), and, more recently, *The Girl with the Dragon Tattoo* (2011).

2005; Holt 2009) have sought to fill this knowledge gap and debunk the myths and stereotypes attached to the hacker subculture, producing taxonomies, looking for motivations, and assessing the significance of hacking in our technology-dependent societies. But only two of these studies (Meyer 1989; Holt 2009) have examined the social organization of computer hackers, emphasizing the existence of cooperative working relationships and their limitations. Nor is it always clear in the above-mentioned studies to what extent respondents are in fact involved in criminal activities.

Surveys and semi-structured interviews (conducted either face-to-face or online) have been the prevailing modes of data collection in this field of research and hacker conventions have been particularly fertile grounds for meeting prospective respondents. The downside of this sampling strategy is that the self-selection process resulting from the decision to attend such highly publicized conferences (Defcon, for example, had 10,000 attendees in 2011) might create a bias toward "white-hat" hackers who feel comfortable mingling with intelligence and law-enforcement agents. Identifying, recruiting, and interviewing informants who are part of the criminal offender population has always presented a number of practical and ethical dilemmas for ethnographic researchers (Hobbs 1995: 2; Shover 1996: 193; Wright and Decker 1997: 3). Academics studying malicious hackers fortunately avoid the risks encountered by those who study armed robbers but the possibility of exaggerated and deceptive responses is substantial.

This chapter seeks to expand our knowledge of the social norms and practices that govern interactions between malicious hackers through a case study based on the seized communication logs of ten confirmed co-offenders. After presenting the data, discussing the types of analysis that were performed, and describing how the material became available to the author, the remaining sections focus on the two variables that define this criminal network's performance: skills and trust. The skills under consideration are the three different sets of cognitive and practical abilities that malicious hackers need in order to succeed financially. Monetization and social skills, in addition to technical skills, play key roles in profit-oriented malicious hacking and explain why earning a decent living in the computer underground remains a laborious endeavour, even for advanced hackers. Trust, which facilitates the diffusion of technical, monetization, and social skills and fosters collaboration, was found to be much lower in this network than is generally assumed in the literature on hacking. In fact, over the two years for which data is available, this network showed significant lacks of trust that erupted into direct aggressions between members without any discernible external pressures to explain this rapid erosion. The need for monetization and social skills as well as the lack of trust between members may partly explain why hacker networks are so ephemeral and vulnerable to law enforcement disruption.

1. Offenders' profiles, data acquisition, and methodology

Before proceeding to a more substantial analysis, it is important to discuss three characteristics of the data. First, the sample of hackers being studied was not self-selected or made up of volunteers met online or at various conferences whose criminal background is hard to authenticate. The hackers involved had been identified by police investigators as suspects in various computer crimes under the Canadian Criminal code, and given this, it was not considered necessary to independently determine the extent of their involvement in malicious and illicit activities. Second, the hackers concerned had been the main focus of an extended police investigation (more than two years), which ended with arrests and equipment seizures that provided a retrospective and unbiased glimpse into their daily routines. Their hard drives were analyzed by investigators in search of evidence and large amounts of data from their communication logs were extracted with the use of advanced forensic tools. Access to these logs means that the data presented here does not depend on respondents' imprecise recollections or hyperbole (Grabosky 2007) but truly reflects their interactions with co-offenders and the evolution of these exchanges. The bias inherent in qualitative interviews about past events is neutralized by access to what amounts to a virtual time-travel machine, allowing private conversations between co-offenders, conducted in an atmosphere free of external interferences, to be reliably captured for systematic analysis. Third, the hackers who make up this sample belonged to the same network, meaning that they had maintained collaborative ties for at least two years. Even if the strength of these ties fluctuated greatly over the reference period, this is, to my knowledge, the first time the inner workings of a hacker network have been studied through a mixed-method approach over such an extended period of time.

In a democracy, such intrusive data can only be collected by a law enforcement organization operating under proper judicial authority. Hence, this research would have been impossible without the support of the Sûreté du Québec (SQ), the national police force for the Canadian province of Quebec. In February 2008, the SQ's cybercrime unit arrested 17 suspects in 12 locations in what became known as Operation Basique. This investigation began in 2005 as an intelligence project looking at the hacking underground, but it soon focused on this particular hacker network when it became apparent that its members operated large botnets of compromised computers. A botnet is usually defined as a group of infected machines under the influence of malware code controlled by an individual known as a "botmaster" (Abu Rajab et al. 2006: 42, Gu et al. 2008: 139). Botnets have been characterized as "compulsory military service for Windows boxes [computers]" (Stromberg cited in Zarfoss 2007: 11), although Apple computers are far from immune (Perlroth 2012). These armies of "zombie" machines are versatile and powerful tools that can be used to launch distributed denial of service attacks, spam and phishing campaigns, and to steal confidential information or carry out click frauds. The largest known botnets, such as Mariposa, Conficker, Rustock, Grum, DNS Changer, or Coreflood, were able to corral millions of machines to their service.

Members of the Basique network did not operate at this level but were nevertheless serious players on the hacking scene. The investigators who analysed their hard drives were able to identify more than a hundred botnets controlled by this group comprising 630,000 IP addresses in 120 different countries. Of the 17 suspects initially arrested, 10 were later charged and all of them eventually pleaded guilty to charges such as unauthorised use of computers, possession and use of passwords, mischief in relation to data, fraud and possession of credit card data. Nine of them were sentenced to periods of home detention ranging from 15 to 18 months, complemented with some community work. One notable exception was the person perceived to be the leader of the group, who received a two-year jail term and three-year probation, possibly the harshest sentence handed down for computer-related offenses in Canadian judicial history. These ten convicted hackers make up the criminal network analysed in this chapter.

The demographic profile of these ten hackers largely agrees with that provided in the literature as all of them were male and their average age at the time of arrest was 20.4 years (range: 17-25). Although only two were minors when arrested, most of the others stated in their initial police interview that they had become interested in hacking as early as eight years old and had become acquainted with botnets by their early teens. Although the sample cannot be considered representative, this particular group seems to corroborate the stereotype of a hacking subculture essentially populated by young males.

Young women appeared regularly in communication logs but as former, current, or potential girlfriends who required technical help or prompted network members to attack people against whom they bore a grudge, never as botnet creators or operators.

This sample differs from typical representations of the hacking community (Turgeman-Goldschmidt 2009: 324) in its involvement in other types of criminal offenses and the occupational orientation of its members. Half of the arrested hackers (5) had previous police records for drug-related offenses (3), theft (2), or assault (2) and were therefore already involved in low-level non-technological crimes. Half of them also repeatedly discussed their drug-consumption habits (mainly cannabis) in the seized logs. Among the five hackers who had steady jobs, only one was employed in the computer industry. The other four worked in trade or manual labour on a family farm, in the logging industry, in a plastics factory, and in a door and window installation company. A sixth hacker was receiving social welfare benefits, although he worked in a variety of undeclared menial jobs. Of the four remaining hackers, two were studying computer science and two had an unknown status. The two features of early involvement in various forms of petty crime and a blue-collar occupational profile contradict the stereotype of the hacker as a computer geek, destined to join the ranks of internet or security start ups after a decisive encounter with the criminal justice system. In this network, hacking was a pastime that provided a sense of freedom and excitement to individuals whose professional and personal prospects were dim. Indeed, three came from dysfunctional families where one or both parents had a criminal record, in some cases for very serious violent offences such as attempted murder. For these individuals, hacking is best described as the extension or diversification of a burgeoning criminal trajectory rather than a misstep in an otherwise uneventful biography.

The original data provided by the SQ consisted of 4,714 one-to-one conversations extracted from the hackers' hard drives, conducted via a synchronous online messaging technology known as IRC (Internet Relay Chat). IRC is a very popular communication tool for hackers, who use dedicated channels to learn new skills, brag about their exploits, and trade illicit goods and services (Franklin et al. 2007). The majority of IRC channels are used by legitimate individuals who appreciate its interactive features (Werry 1996). Hackers themselves frequently use IRC for purely social purposes. For example, while the 4,714 conversations mentioned above involved 761 individuals (in addition to the 10 hackers), 95.1% of these users were apparently not involved in illicit activities (Décary-Hétu and Dupont 2012) but were friends and family members or complete strangers with a common hobby. The seized logs also included public discussions that took place on freely accessible hacking channels and implicated numerous individuals in illegal hacking activities, but offenders are aware that these channels are monitored by law enforcement agencies and usually avoid implicating themselves. Such forums act more as meeting points that provide initial contacts which can then be followed up by private conversations. In order to focus on the most serious content and avoid being drowned in large volumes of useless data, it was decided to restrict the analysis to private IRC discussions between the 10 arrested hackers (which yielded 113 chat logs) and between these hackers and other individuals if conversations contained certain keywords or technical references suggesting malicious activities (89 additional chat logs)[3]. Overall, 202 text files containing almost a quarter of a million words (243,978 to be precise) were coded and analyzed in order to understand how this network operated. A qualitative data analysis software called QDA Miner facilitated the coding, annotating, and retrieval of this large dataset. The social network analysis

[3] These keywords were chosen to capture the most frequent terms associated with botnet, DDoS, carding and fraud activities.

component of that project relied on the UCINET software package (Borgatti et al. 2002). In order to maintain the privacy of the arrested hackers and their interlocutors, an identifying number was randomly allocated to each discrete nickname extracted from the IRC chat logs.

Although these logs represent only a fraction of the data seized by investigators (0.01% of the 348MB of text files retrieved from the hackers' hard drives), their content can confidently be characterized as the most informative. IRC channels are routinely used by botmasters to receive information from and send commands to machines they have infected all over the world (Stone-Gross et al. 2009) and a large number of the remaining logs contained automatically generated lines of computer code that are of little value for the purpose of this research.

The data under consideration must obviously be interpreted with care, as it may suffer from a number of biases. The chats logs could have been erased at regular intervals by security-minded hackers in order to suppress evidence in case of an arrest, reducing our ability to grasp the true extent of these prudent offenders' skills. But in order to be completely effective, this precaution would need to be taken by each of the individuals concerned, which is rarely the case. Logs might also have been erased involuntarily as the result of a hardware failure and a lack of backup, unfortunate incidents that can strike even the most proficient hackers. Alternatively, the recent purchase of new equipment might mean that all archived data in old machines had been disposed of and thus was unavailable for further analysis. As well, identification of individuals was not always straightforward. While it was sometimes possible in the qualitative analysis to uncover instances where an arrested hacker had used multiple nicknames and his various numerical identifiers could thus be recoded, this process could not be implemented for all protagonists and the same person could very well be represented as multiple nodes (one node per nickname). Finally, the timestamps used to record the day and time at which online conversations occurred were automatically assigned by the hackers' machines, but a de-synchronized or incorrectly set internal clock could distort the chronology of events. With these caveats in mind, we can proceed to the first stage of the data analysis and consider the level of expertise demonstrated by these hackers as well as the different types of skills exhibited by network members.

2. The unequal distribution of technical, monetization, and social skills

As explained previously, botnets are versatile and powerful illicit tools that can provide significant profits to their operators. A number of empirical studies relying on leaked or manipulated data from command and control (C&C) servers used to coordinate large armies of compromised computers have estimated that the most successful botmasters generate revenues of up to US$3.5 million per year, mostly from spam sent on behalf of online pharmacies (Anderson et al. 2012, McCoy et al. 2012). However, researchers have found that profits are much more modest for the majority of bot herders, whose median incomes range from a few hundred to a few thousand dollars a year, depending on their strategies (Herley and Florêncio 2009, McCoy et al. 2012). So, despite media and industry reports that stress the ease with which botnets can be purchased or rented online (Ollmann 2008, Danchev 2010, Krebs 2011, Leyden 2011), most hackers still find it difficult to benefit financially from this widely available technology. The economics of botnets and underground markets certainly explain in part why it is so hard for botmasters to turn a profit (Herley and Florêncio 2008, Anderson et al. 2012), but I suggest that considering the mix of skills that botmasters possess or lack is also important in understanding their success or failure. Using the typology developed by

Copes and Vieraitis (2008) for identity thieves, malicious hackers who want to succeed financially need three types of skills: 1) technical, 2) monetization ("system knowledge" in Copes and Vieraitis's terminology), and 3) social. Consideration of how the arrested hackers performed, individually and collectively, in each category shows that technical skills are crucial but not sufficient, and that monetization and social skills are in much more limited supply than technical skills.

a. Technical skills

In the context of this particular hacker network, technical skills are the technical expertise or knowledge that can be mobilized for the development, deployment, and maintenance of a large pool of stable and stealthy robots. While the most talented hackers are able to create original botnets, most botmasters prefer to download existing malicious code from various internet forums and modify these generic applications in order to suit their needs. Many "families" of botnets have evolved over the years and share a common codebase, with new extensions and functionalities constantly added, the most popular being Agobot, SDBot, SpyBot, or GT Bot (Barford and Yegneswaran 2007). The arrested hackers favoured SDBot and variants such as JrBot and RxBot, as well as a rarer type of bot known as Kaiten. According to the Honeynet Project, a non-profit security organization that investigates computer attacks, none of these two botnet families are considered particularly sophisticated (Bächer et al. 2008). Both have been widely available since early 2000, which suggests that the arrested hackers preferred to deal with more established "products" for which there are numerous online tutorials. The arrested hackers' machines revealed no trace of the more elaborate ZeuS botnet, which is specifically designed to harvest online banking credentials and appeared in the wild as early as 2007 under the name NTOS (Lemos 2010), a clear indication that our hackers do not fit the “early adopter” or “innovator” profiles.

Of the 10 hackers, one stood out as the technical leader of this network. N378 was able to significantly modify the malware codebase he downloaded from the internet. He was also very effective at propagating his malicious code and at the time of his arrest he controlled almost half the compromised machines infected by this network (291,000 bots). His technical expertise was undisputed among other network members, and he acted as a mentor and teacher for less technically advanced hackers. He also shared some of his custom-built code and, in a few instances, provided access to the C&C servers that controlled his bot army to let co-offenders use his attack capabilities. Police investigators claim that he had used this technical expertise to launch 153 DDoS (denial of service) attacks over the two years preceding his arrest and more than 2,000 passwords and 500 credit card numbers were in his possession when he was arrested.

The remaining members of this hacker network were much more modest in their technical prowess, with a median number of 60,197 controlled bots, and a low of 314 infected machines for N142. If these hackers were avid attackers, their technical skills limited their ability to steal credit card numbers and banking credentials from their victims. A good example is N286, who controlled 104,000 bots but had only managed to obtain nine credit card numbers. These hackers also found it difficult to maintain their infrastructure, as their bots and C&C servers, which were all hosted on compromised machines, were frequently detected and removed by their victims. On a number of occasions, N1 and N142 lost all of their bots in this fashion and turned to N378 to ask him to spare a few of his bots so that they could immediately resume their activities (a request that was denied in both instances).

The uneven distribution of expertise among network members did not seem to be compensated for through the purchase or rental of easy-to-use malware packages -- what security industry analysts call the “malware as a service” model, where, for a fee, malware developers offer aspiring slow or lazy hackers advice, technical support, and money-back guarantees as well as upgrades (Gilman 2009). None of the network members operated the types of botnets found for sale on underground markets (such as ZeuS) and their socio-demographic profiles suggest it is unlikely that they would have had the necessary funds for such an investment as some of the most sophisticated malware kits can cost up to a few thousand dollars (Stevens and Jackson 2010).

The technical skills required to set up and operate a large botnet are far from insignificant and only those ready to invest significant amounts of time or money can move beyond an initial experimentation phase. Talent also plays an important role and, above a certain level of complexity, motivation alone is not sufficient to acquire the necessary skills. This is not to say that hackers who display rudimentary technical expertise cannot cause substantial damage to computer systems, as the activities of this network make abundantly clear, but these apprentices are largely empowered by mentors who tend to shape their network’s technical capability. Finding and removing these few technical leaders is likely to be one of the most reliable ways to disrupt hacker networks, as they are difficult to replace.

b. Monetization skills

Knowing how to conscript thousands of vulnerable machines will allow a hacker to carry out attacks against an adversary’s computer system or to steal banking credentials, but in order to convert these abilities into income, a second category or skills is required. Copes and Vieraitis (2008: 102) define system knowledge as the "understanding [of] how banks and credit agencies operate and ... which stores require identification." The characterization of monetization skills used here involves a broader range of knowledge that includes—but is not limited to—the approximate value that various bits of stolen information can fetch on underground markets, the online forums where stolen data can be traded, botnets can be rented, or co-offenders can be recruited in order to siphon credit card and bank accounts, the alternative financial tools that govern money transfers between illicit actors (who do not accept credit card payments), and the informal rules that govern these exchanges and protect dealers against the numerous "rippers" who haunt these markets (Herley and Florêncio 2009, Motoyama et al. 2011), as well as the security procedures that are implemented by online and brick-and-mortar retailers or banking institutions in order to prevent fraud and account takeovers (Newman and Clarke 2003).

Although the most capable members of this network displayed technical skills above the script-kiddie level, they were very limited in their monetization skills. Even N378, the network's technical leader, who sorely needed money, experienced difficulties in converting apparently straightforward opportunities into cash, as the following discussion with N1077 (who was not a network member) illustrates:

> [23:38] <1077> I have 18 cards waiting
>
> [23:38] <1077> I send you 500$ by WU [Western Union, one of the preferred money transfer solutions among internet fraudsters] for each card that works as expected
>
> [23:38] <1077> 2k cash and 2k shopping
>
> [23:38] <378> lol [laugh out loud]
>
> [23:38] <1077> I cashout 1k for the card's owner
>
> [23:38] <378> this is another business

[23:39] <1077> I end up with 500 and you too

[23:39] <378> today

[23:39] <378> the police

[23:39] <378> seized

[23:39] <378> my car

[23:39] <378> for the second

[23:39] <378> time

[23:39] <378> this month

[23:39] <1077> lol why

[23:44] <378> you need the login

[23:44] <378> the password

[23:44] <378> social insurance

[23:44] <1077> wooo

[23:44] <1077> no

[23:44] <1077> I don’t have this

[23:44] <378> just the last 3 numbers

[23:44] <378> and his birthdate

[23:44] <378> and the account needs to be activated

[23:44] <378> I hope you knew that..?

[23:44] <1077> I tell you I have the card with the embossed numbers and the dob [date of birth] that’s it I know a guy who is able to do all this with the info I have

[23:45] <378> otherwise the transaction will not proceed

[23:45] <1077> I only have the card and the pin and the dob that’s it

[23:46] <378> ahhhhhh

[23:46] <378> you want to offer me some cashout

[23:46] <378> LOL

[23:46] <1077> I try to find another guy who can do the same things as my former guy

[23:46] <1077> I want you to hack a bank account then put some cash on my card and I will cash it out

```
[23:47] <1077> that's it

[23:47] <1077> so can you still do it

[23:47] <378> well we would have to spam

[23:47] <378> and that is more preparation

[23:47] <378> you need to hack a website

[23:47] <1077> i know

[23:47] <378> you need to host a page

[23:48] <378> I think I have one in backup

[23:48] <378> give me two seconds to check

[23:48] <1077> 2k if you can do it I give you 500$

[23:48] <1077> per card

[23:48] <1077> that works

[23:48] <378> r you crazy

[23:48] <378> its 50 50

[23:48] <1077> well that’s it

[23:48] <1077> lol

[23:48] <1077> 500/500

[23:48] <378> then you have 500 for the cost of the card

[23:48] <378> lol

[23:48] <378> your funny man

[23:48] <1077> because of the card owner I give him 1000$

[23:48] <1077> and I cashout 2k

[23:48] <1077> max

[23:49] <378> we can cashout

[23:49] <378> more than 2000 man

[23:49] <378> we can use the card

[23:49] <378> 2 3weeks

[23:49] <1077> before he realizes ?

[23:49] <1077> you think ?
```

[23:49] <378> yes

[23:49] <378> I am sure of it

[23:49] <378> you find a 10k account

[23:49] <378> you think you take just 5k$

[23:49] <378> but the account has to be activated [for online transfers]

[23:49] <378> its more difficult

[23:50] <1077> look my guy before I gave him the card and the dob and he came back the following day with cash

[23:50] <378> you need to call the bank to activate the accounts

[23:50] <1077> i know

[23:50] <378> and to start this

[23:50] <378> I need to do some work

[23:50] <378> I don't have spamming lists anymore

[23:50] <378> I don't have a spammer either

[23:50] <1077> damn

[23:51] <1077> so … what does it mean you can't do it ?

[23:51] <378> hey fatso you think I don't have a life and I spend my time defrauding banks

[23:51] <1077> well 2k you'd be rich hehe

[23:51] <378> it means I need some more stuff before I become operational

In this conversation, N1077, who has heard of N378's hacking reputation, offers to allow him to take the place of a previous technically savvy co-offender, whose fate is unknown, in initiating money transfers to bank accounts whose owners have sold him their debit cards. Although the owners pretend to be the victims of this fraud, they receive a share of the profits from N1077. N378's role is to hack into other bank customers' accounts (the real victims in this case) in order to initiate intra-bank transfers to the debit cards held by N1077. However, what initially seems simple to N1077 never happens and the discussion carries on for a few more days without any tangible outcome, as N378 always finds a technical pretext not to follow up on N1077's offers. This conversation took place at a time when N378 could have used the money to pay outstanding traffic fines and recover his seized car. What prevented him from exploiting the stolen debit card numbers was not some form of higher hacker ethic but a lack of familiarity with common fraud schemes, as can be seen in the following log excerpt:

```
[23:35] <378> hey man
[23:35] <378> have you ever fiddled with cc [credit cards]
[23:35] <378> because I just coded a new sniffer for my worm [a computer program that
          intercepts data and passwords between computers]
[23:35] <378> and I tested it
[23:35] <378> and it looks crazy
[23:35] <378> 125ko
[23:35] <378> .txt [refers to text files]
[23:35] <378> all cc
[23:35] <378> all fuken fresh
[23:35] <378> what the fuck do I do with that
[23:35] <378> I just know [name of his local credit union]
[23:35] <378> and not very well
[23:36] <852> weird I thought that cc required SSL encryption [a protocol to protect
          information when it travels on the internet]
[23:36] <852> well … cc are touchy … you need to find some kind of abandoned place where
          you can have things delivered…
[23:36] <852> a drop site
[23:36] <852> or else, you'll be caught instantly
[23:36] <852> and you need to avoid surveillance cameras that could film who is picking up
          the stuff …
[23:36] <852> it's shit as far as I am concerned
[23:37] <852> I would trade them on carding sites against whatever
```

[23:37] <852> You're more likely to end up in jail than anywhere else with these

[23:37] <852> or else, you can use anon proxy [an anonymous proxy to mask one's identity when surfing the internet] to create legit shells… or xxx websites access

[23:37] <852> that kind of shit

[23:38] <378> yep

[23:38] <378> but a shell is no better

[23:38] <378> you must not use your real IP [Internet Protocol address, a unique identifier assigned to each machine connected to the internet]

[23:38] <378> but I know something

[23:38] <378> my chum works in a store

[23:38] <378> he says you need cc

[23:38] <378> and the expiry date

[23:38] <378> and he can get a lot of stuff out

[23:38] <378> I will check it out

[23:38] <378> I have like

[23:38] <378> of lot of cc

[23:38] <378> and it increases every day

[23:38] <378> my sniffer has gone wild

[23:38] <378> check it out

In this conversation, N378, the technical mentor, turns to an outsider for advice on monetization strategies. Indeed, a keyword search through N378's entire logs reveals only one successful cash conversion, which was a fairly modest achievement, as can be seen in the following discussion with another network member.

[18:27] <378> fatso I was in a bind in Quebec City

[18:27] <378> the day before yesterday

[18:27] <378> really in deep shit

[18:27] <134> why

```
[18:27] <378> I carded a motel
[18:27] <378> some pizza
[18:27] <378> red wine
[18:27] <378> smokes
[18:27] <378> LOOOOl
[18:27] <378> can’t imagine how easy it was
[18:27] <134> loll
[18:27] <378> no need for cvv [Card verification value, an anti-fraud security feature]
          nothing
[18:28] <378> #carte exp: [expiration date] name of cardholder that’s it
[18:28] <378> and pizza was the easiest
[18:28] <378> are you hungry?
[18:28] <134> lol
```

Being a skilled hacker does not equate with being a skilled fraudster, and controlling a large botnet that can harvest thousands of credit card numbers does not automatically make someone rich without some significant additional skills and a willingness to take some risks in the physical world. Despite his technical mastery, N378 experienced regular financial difficulties, as he made clear in the first excerpt in this section, and it is perhaps not surprising that his highest profile DDoS attack was in retaliation against the servers of the bailiff who seized his car. None of this network’s other members seemed to have developed strong monetization skills, and the largest proven gain discussed among them included the sale by N1 of a thousand bots to an undisclosed buyer for $300. The lack of monetary sophistication shown by this network can also be seen in their preferred method of payment, which involved direct bank transfers to their accounts, which were with the same bank that was the main target for their phishing campaigns. While there are a few skeptics (Herley and Florêncio 2009, Anderson et al. 2012), most of the limited literature on hackers assumes that large botnets automatically generate matching revenues, but, as shown here, such a positive correlation cannot always be inferred. When technical and monetization skills reside in different parts of—or even outside— the network, social skills must be mobilized in order to establish a connection.

c. Social skills

In their research on identity thieves, Copes and Vieraitis (2008: 100) define social skills as the "ability to manipulate the social situation through verbal and non verbal communication." In the online context, manipulation takes place primarily through technical means and social skills therefore play a less central role in offender-victim interactions. They are, however, crucial in the search for suitable co-offenders who possess the required technical or monetization expertise, since traditional meeting opportunities such as residential proximity, leisure activities, or prison (Tremblay 1993) are not as abundant for cybercriminals. The required social skills include the ability to establish and maintain productive interpersonal ties through computer-mediated communications with trustworthy accomplices they have never met in person, who must not only possess the needed qualifications but also refrain from defecting from established relationships. Social skills are as much a matter of quantity as of quality: a large number of contacts with a broad range of diversified skills is obviously one of the principal outcomes of social skills, but these contacts must also be available on short notice with minimal negotiation (in order to lower transaction costs) and must be sufficiently reliable to avoid malfeasance, mistakes, or failures (Tilly 2005: 6). The ability to generate and cultivate trust among co-offenders is thus a strong qualitative indicator of one's social skills.

Valued graphs are well suited to measuring the varying strength or intensity of interpersonal relationships (Freeman et al. 1991: 144-145; Wasserman and Faust 1994: 140), and identifying prominent actors who seem to exhibit stronger social skills than their counterparts. In our sample, each conversation was coded as one interaction; table 1 shows the number of interactions by each hacker with other network members and each actor's percentage of interactions within the overall network during the two years that preceded his arrest. N1 appears to be the most active member in this network, as he accounts for more than one third of intra-network interactions (37.6%), while N378, who has already been mentioned as the most technically competent hacker, comes second with 22.1% of exchanges.

Table 1 goes about here

Using a second type of centrality measure that does not focus exclusively on direct ties but also takes into account the brokerage role of a node – its capacity to relay information between two nodes – shows that N378's social skills remain lower than might be expected, as N1 has the highest flow betweenness centrality of all his counterparts, and two other players (N516 and N286) have higher or similar scores to N378. However, despite being by far the most central actor in this network, according to the investigator's records N1 controlled only about 47,000 bots,[4] far behind N378 (290,000 bots), N121 (122,000 bots), or N516 (77,000 bots). This disconnect between social and technical activities may to a certain extent reflect a protective strategy designed by N378 in order to insulate himself from asymmetrical demands from less competent hackers who could never reciprocate his assistance. In this particular kind of

[4] The number of compromised IP addresses is usually about half the recorded signatures, as hackers tend to experiment and to infect the same computers with different bots. For a more detailed discussion of the impact of differing botnet measurement methodologies on the assessment of the problem, see Abu Rajab et al. (2007).

network it is important to recognize that social leaders (such as N1) can be distinct from technical leaders (such N378) or even business leaders (none in this case), and that attempts to disrupt the network will have slightly different outcomes depending on the type of leadership that is targeted.

So far, the main metric used to derive a ranking of the most central actors in this network has been the number of discussions. But social skills are as much about quality as about quantity, a feature that is hard to measure without conducting a content analysis of the conversations. Figure 1 uses the centrality measures computed above to represent the hacker network: the more frequent the interactions, the thicker the line used to visualize each tie. Figure 1 suggests that the two most significant relationships are the N378-N1 and the N1-N516 dyads, but examination of the content of these discussions clearly indicates that these partnerships did not always run smoothly and could very easily turn sour.

Figure 1 goes about here

Therefore, in the following section I complement the traditional social network analysis indicators of centrality and brokerage with a qualitative approach that seeks to determine what conversations were actually about. In this particular case, frequency of contacts is a poor measure of relationship strength, as conflicts between individuals present patterns of intense communication that look very similar to privileged connections.

3. Distrust and hostility among network members

In order to determine the levels of trust that linked the members of this network, each conversation in the dataset was coded using the qualitative software QDA Miner. Additional data provided by the investigative team, such as the profiles of arrested hackers prepared for the local detectives who conducted the first interview, was also taken into consideration. The goal of this exercise was to determine, for each pair of hackers, the quality of their relationship at two different periods, the years 2006 and 2007. The qualitative analysis uncovered three main types of links: high-trust relationships, which involved unconditional cooperation between members on various projects and even a level of personal intimacy; low-trust relationships characterized by systematic cost-benefit analysis in order to determine for each demand the amount of assistance to be provided; and hostile relationships, where insults, threats, and frequent attacks were the main modes of interaction.

Figure 2 goes about here

Figure 3 goes about here

It is possible to visualize the evolution of these ties over time by representing each relationship according to its level of trust, with solid lines indicating high-trust ties, broken lines reflecting low-trust ties, and dotted lines indicating hostility. Comparing figures 2 and 3 makes it easy to locate resilient alliances or decaying partnerships, but it is difficult to assess how each hacker handles the three types of relationships and which individuals have more collaborative—or conflictual—tendencies. Table 2 attempts to provide a more comprehensive overview of this network's stocks of individual and collective social capital and liabilities by showing the distribution of high-trust, low-trust, and hostile relationships for each hacker for the years 2006 and 2007. Arrows in the right-hand column indicate the upward, downward, or lateral evolution of these relationships.

Table 2 goes about here

The bottom line of the table suggests that the proportion of high and low-trust relationships decreased significantly from the first to the second year, with hostile relationships between several members representing one third of interactions at the time of arrest. In absolute terms, high-trust relationships remained constant but the relative value of these relationships for the network as a whole was diluted by an increase in the number of hostile interactions. From 2006 to 2007, this network, which started as a high-trust environment, morphed into a web of distrust. In the following paragraphs, I examine the causes of this shift and its consequences for cooperation by analysing each type of relationship.

a. High-trust ties and cooperation

As discussed previously, network members displayed diverse levels of technical expertise. Hacker networks are principally involved in knowledge transfer, with the most talented members imparting knowledge, either explicitly or implied, to newcomers or apprentices deemed worthy of it. More rarely, members of a hacker network will conduct a joint operation, coordinating their activities to attack a target or pooling their resources for a specific task, such as testing the effectiveness of a newly coded program (Holt 2009).

In this particular network, members who trusted each other exchanged information on how to obtain, modify, and operate certain malicious applications, collaborated in order to solve technical problems (such as the instability of the bots they were using), shared pieces of code they had written, let others access their servers by sharing their login and passwords, or warned each others about behaviour that might attract the attention of governmental authorities. For example, N378 warned another network member against scanning IPs in range 140, which is largely allocated to military computers and is used by the US Defense Information Systems Agency and Fort Bragg, the home of the US Army Special Operations forces. N378 advised his apprentice to confine himself to more benign ranges such as 128, 129, and 130, which belong to educational institutions. In another instance, whose irony seemed to escape both protagonists, N516 asked N378 which would be the most effective anti-virus solution on the market to protect his mother's laptop. Here is N378's response, which he promised would make the computer "un-hackable":

```
[21:51] <378> what is the os [operating system]
[21:52] <516> p4 centrino
[21:52] <516> win xp
[21:52] <378> xp ?
[21:52] <378> k
[21:52] <516> yeah
[21:52] <516> like 1.76 ghz
[21:52] <516> 1 gb ram
[21:52] <378> you install her sygate for xp pro
[21:52] <516> yeah
[21:52] <378> as a firewall
[21:52] <516> sygate that's what I thought
[21:52] <378> you fetch adware ligit
```

```
[21:53] <378> a small anti virus
[21:53] <378> nothing too heavy
[21:53] <378> that only does the essential
[21:53] <378> like panda platinum
[21:54] <516> fuck it
[21:54] <378> with the permanent protection file
[21:54] <516> this is shit
[21:54] <516> lol
[21:54] <378> nah not that bad
[21:54] <378> mine yes
[21:54] <378> bcse it’s old
[21:54] <516> ok
[21:54] <378> but they are not listed anywhere panda
[21:54] <516> ok
[21:54] <378> because
[21:54] <378> with these three tools
[21:54] <378> she cannot get hacked man
[21:55] <378> you have iptables firewall
[21:55] <378> a registry blocker
[21:55] <378> a permanent protection file
[21:55] <516> ok
[21:55] <378> a small antivirus that does the job and that is not annoying when it finds a virus
[21:55] <516> ok good
[21:55] <516> thx:)
```

Not all discussions were task-oriented and high-trust ties also implied that the long and dry technical exchanges would be interspersed with discussions of personal issues:

frayed relationships with girlfriends or family members, lack or loss of employment, financial difficulties, weekend plans, and drug use were discussed between certain pairs of hackers and broke the monotony of computer programming and botnet management. These personal confidences were probably instrumental in creating rapport and reinforcing social ties between people who had never met in person, and whose social costs for defecting would therefore have been very low, if not null.

b. Low-trust relationships and contingent cooperation

High-trust relationships never comprised more than 56% of network ties and the two dyads with the most frequent interactions (N1-N378 and N1-N516; see figure 1) were characterized by limited levels of trust from the start. In low-trust relationships hackers exchanged information and shared resources only up to a certain threshold, beyond which cooperation was suspended or withdrawn. This more closely controlled flow of information and resources was generally the result of either the disparaging attitude displayed by more technically skilled hackers towards less qualified members of their entourage or a specific incident that led one hacker to question the reliability of another network member.

For example, N378, the master hacker and unofficial mentor in this network, explained to N834 (an outsider who said he earned more than $10,000 a month through credit card fraud) why he limited his collaboration with other network members:

```
[06:47] <378> I don’t want to help anyone
[06:47] <378> for bots
[06:47] <378> each time I help someone
[06:47] <378> my worms stop working
```

```
[06:47] <378> since I stopped helping people
[06:47] <378> my worms are on fire
[06:47] <378> all those I help leech my codes
[06:47] <378> and leak it everywhere
[06:48] <834> don’t worry, I am not like that
[06:48] <834> you know me better
[06:48] <378> so, I am fucking tired that everything I do is leeched but that I am considered
        as a fucking noob [an inexperienced person who has no will to learn in hacker
        jargon]
[06:48] <834> agree
[06:48] <834> accept the dcc send [An IRC code that allows users to send and receive files]
[06:48] <378> but everyone comes to see me when it’s about bots
[06:48] <834> hehe your not noobs man
[06:48] <834> you’re wiser than me
[06:48] <834> I can’t even code a fucking bot
[06:48] <378> msn
[06:48] <378> well its tough man
[06:49] <378> I have been at it for years practicing coding worms
[06:49] <378> just doing that all the time
[06:49] <378> collect sources for bot packers and whatever
[06:49] <378> meanwhile I collect all kind of stuff
```

In this discussion, N378 describes how asymmetrical he feels his interactions with other hackers are: while he is being asked a lot of technical questions and even to share his proprietary malicious applications, he gets very little (not even the respect he believes he is due) from those interactions. This attitude reflects a very individualistic approach to hacking: far from seeing himself as a group leader, his mind-set is more that of a craftsman – his skills have been acquired through trial and error and personal sacrifice and as a result should not be made available to people who are not ready to invest the same amount of time and effort. This lack of trust not only limited the network's technical effectiveness but also restricted its monetization opportunities. In a follow-up discussion between N378 and N834, the former explains that he does not trust money transfer services such as Western Union, which are very popular with internet fraudsters (Tyler et al. 2009), and prefers face to face cash exchanges. This type of attitude was unlikely to facilitate the integration of the network with international fraud rings that operate at the transnational level (McCusker 2007) and rely on virtual currencies and money transfer services to pay their associates and repatriate criminal proceeds.

A second source of low-trust interactions results from specific instances of malfeasance, mistakes, or failures (Tilly 2005). In the following excerpt, N378 denies N1's request to share some bots, justifying his decision by an operational mistake made a few years earlier that has never been forgotten:

[12:37] <1> do you think you would be able to download me some bots to help me out and I will help you back when you want

[12:38] <378> no lol

[12:38] <378> I gave you some a while back

[12:38] <1> you took them back

[12:38] <378> you did not keep them

[12:38] <1> it was 2 years ago

[12:38] <378> nah never

[12:38] <378> I gave them to you

[12:38] <378> you did not know how to keep them

[12:38] <378> it was 5 years ago

[12:38] <1> my exe [executable file] was detectable and not packed [compressed with a specific application in order to hide the file's true content] then

[12:39] <378> I have the same bots

[12:39] <378> and you're wrong they were packed

[12:39] <378> you had mew11

[12:39] <378> lo

[12:39] <1> no I had the small aspack [an executable file compression software]

[12:39] <1> it was not very good

[12:39] <1> and now they are packed and undetectable

[12:40] <1> I did not know anything then now I know better and I know how to keep them

In the end, N1 did not sway N378. A subsequent discussion about N1's alleged predatory behaviour did not do anything to allay N378's distrust of N1's motives:

[15:59] <378> he man

[15:59] <378> did you steal N519's bots by any chance

[16:01] <1> nah I told you I removed all mines

[16:01] <1> I give up that shit

[16:02] <378> dude he says that when he logged on his server

[16:02] <378> he had 79 bots left

[16:02] <378> and that you left just after

[16:02] <1> I know he told me the same

[16:02] <1> and I told him I crashed as well

[16:02] <378> in any case man

[16:03] <378> a couple of people told me you were after their bots

[16:03] <1> I will not touch anything why don't he fixes his bots

[16:03] <1> and even if I am after their bots all bots are mine N121 and N519 would never had any bots without my help

[16:03] <378> last thing

[16:04] <1> but anyway I don't give a shit I gave up for good

[16:04] <378> when you accuse someone

```
[16:04] <378> make sure
[16:04] <378> you can prove what you say
[16:04] <1> anyway I am going to the beach
[16:04] <378> I have broad shoulders but there are limits to what I will tolerate
```

These low-trust interactions do not paralyse the network, as superficial or low level forms of cooperation can still take place, but the higher transaction costs they create certainly curtail its effectiveness. A lot of pleading and cajoling is required to overcome the underlying distrust and the constant reassurance that must be provided to certain members does not always guarantee a positive outcome. Another consequence of the limited supply of trust within this network is reluctance to engage jointly in riskier (but potentially more rewarding) projects, as new initiatives are met with suspicion and skepticism, not the best way to foster innovation. The constraints and instability imposed by the high proportion of low-trust interactions among some of the network's most central members can culminate in the quick deterioration of relationships. Hackers are then entirely or partially excluded from the network and as a result must dedicate an inordinate amount of time to conflict management.

c. Friend to foe: the enemy within

Toward the end of the second year, N121 and N142, who had been on the periphery of the network during the previous year, were locked into hostile relationships with the rest of the network and seemed to have exhausted the limited trust that had been extended to them. They were not, however, completely disconnected from the network, as they remained technically able to repeatedly attack their former allies' machines and servers. The same sequence led to these outbreaks of hostility. Both N121 and N142 had initially collaborated on a limited basis with N1, while N378 had imparted some of his knowledge to N142. But after a year of low-trust interactions, accusations were voiced about the careless handling of shared resources that had been lost to the group, and insults about selfishness and lack of support from the more experienced hackers became more common. It was not long before the technical and social leaders lost their patience and decided to make an example of N121 and N142, using their powerful botnets to launch repeated attacks against them. N121 and N142 refused to be intimidated and retaliated. The escalation of this conflict culminated with N1 and N 142 receiving death threats on the phone.

This rapid decay of trust leading to the exclusion of some network members is not a marginal trend, as by the end of the second year more than 28% of the network's relationships can be classified as hostile. Such a sharp increase (from 0% the first year) is produced by the deterioration of low-trust partnerships and the spread of disputes to hackers who were not involved in the original arguments. By contrast, high-trust relationships demonstrated their resilience, as none of them suffered any deterioration during the reference period. However, in less than 24 months, this network, which had not (yet) been exposed to police action and was free to operate unrestrained, spontaneously became unstable and lost some of its effectiveness. This self-created fragmentation made the network dysfunctional and significant resources had to be diverted from hacking projects and allocated to minimize the fallout from these incidents.

This situation is radically different from the Caviar drug importation network studied by Morselli and Petit (2007), which remained operational despite the erosion of trust caused by recurring seizures of hashish and cocaine consignments. Faced with signs of mistrust between network members following one of the first police disruptions, that network leader tried to remain cool-headed in a telephone intercept with an associate: “I’m trying to put things back on the road. I’m trying to save all this aggravation because, if it’s gonna come to that, it’s gonna be a mess and it’s the last thing I want for you and for everybody, I just wanna fix this up diplomatically” (Morselli 2009: 95). By comparison, diplomatic skills were in very short supply in the hacker network under study, where random acts of aggression were often observed, fuelled by a potent mixture of boredom and touchiness. In the following excerpt, N378 and N564, who share a low-trust relationship, discuss potential targets for N378’s bots, which are online but idle.

[15:03] <378> do you have someone

[15:03] <378> to flood [an attack that consists in sending data faster than the receiver can process, which causes the target to disconnect from the network]

[15:03] <378> I have 900 proxy

[15:03] <378> online

[15:03] <378> lol

[15:03] <564> no

[15:03] <564> but… don’t flood [name of third hacker]

[15:03] <564> he’ll be crazy hahaha

[15:03] <564> I’ll find you someone to flood

[15:03] <564> fuck

[15:03] <564> [name of a fourth hacker] is not online

[15:03] <564> it stinks

[15:03] <378> lol

[15:03] <564> lol

[15:03] <378> wait

[15:03] <378> until he sees it

[15:03] <378> I flooded him

[15:03] <378> with 60 bot

```
[15:04] <378> now I have 800
```

When N564 attempts to clarify the reasons behind this attack, the answer he receives is laced with veiled threats. While attempting to deflect the planned assault against the third hacker, he keeps looking for a suitable alternative target.

```
[15:09] <564> why do you flood him exactly?
[15:09] <378> its a request
[15:10] <564> who from?
[15:10] <378> hahaha
[15:10] <378> you just saw me
[15:10] <378> on the chan
[15:10] <378> shut up
[15:10] <378> or I flood you
[15:10] <378> :P
[15:10] <564> yeah
[15:10] <564> i know
[15:10] <564> hahaha
[15:10] <378> hahah
[15:10] <378> nah i mess around
[15:10] <378> but man
[15:10] <378> I have 800 prox
[15:10] <378> online
[15:10] <564> take it easy
[15:10] <378> do you have someone
[15:10] <564> stop flooding him
[15:10] <378> that i hate
[15:10] <564> he’s gonna eat crap
```

The lack of maturity displayed by network members,[5] combined with the availability of powerful tools that can be used for malicious actions, explains to a certain extent why already fragile low-trust relationships easily descended into open conflict. But the volatility of these ties can also be ascribed to structural features of the internet: the capacity to shed one's online identity at will and adopt new nicknames when a reputation is damaged, the unlimited pool of potential co-offenders who can be met online on dedicated underground forums and IRC channels, and the limited opportunities imposed by geographical distances and anonymity on the use of physical coercion as a compliance and control mechanism all contribute to lowering the costs of malfeasance and betrayal and to exacerbating distrust, a latent attitude among delinquents (Tremblay 1993: 25). In that context, we should not be surprised to see such a high rate of infighting among network members.

Conclusion

Neither super-empowered technicians (Ohm 2008) nor socially inept teenagers, malicious hackers face practical challenges that are very familiar to more traditional offenders. Finding suitable and reliable associates with a broad range of complementary skills is a time-consuming quest that often has inconsistent outcomes. Although technical skills have been the main focus of most empirical and theoretical studies on hackers – along with the complex issue of what motivates them (Taylor 1999, Schell et al. 2002, Rogers 2006) – I hope to have made a persuasive argument for the need to conduct more empirical studies on the equally important monetization and social skills.

[5] For example, one hacker, upon entering the courtroom where he would have to convey his plea to the judge, raised his handcuffed hands as if he had just won a sport competition and smiled at press photographers.

Malware monetization strategies are being researched by computer scientists, using concepts borrowed from the economists' toolbox (Moore at al. 2009), but we still need to understand what constraints are at work, how opportunities are structured, and how decisions are made from a hacker's perspective (Reuter 1983). The hacker network discussed here, for example, was never able to acquire monetization skills, despite the precarious financial situation of one of its leaders and his control of significant computer resources.

The social capital that flows through such technology-mediated criminal networks also deserves much closer scrutiny. The scientific literature has, in my view, overestimated the ability and willingness of hackers to collaborate (Taylor 1999: 62, Schell et al. 2002, Holt 2009), assuming that the convergence of the global proliferation of available communication platforms, the semi-anonymity afforded by these technologies, and the jurisdictional boundaries constraining law enforcement agencies have eliminated the barriers that traditionally constrained illicit markets. However, far from creating a frictionless social environment for malicious hackers, these digital tools have a darker side that, under certain conditions, hinders collaboration and fosters distrust.

As online or seized data becomes increasingly available to researchers and computational social science methods allow them to process and analyze massive amounts of data (Lazer et al. 2009, and, for the methodological and ethical limitations of this approach, see Boyd and Crawford 2011), unique opportunities to study the social organization of malicious hackers open up. The data presented in this chapter suggest, for example, that a hacker network that controls large botnets and does not use them for fraudulent (or political) purposes will be tempted to turn this unused firepower against some of its close associates or even those in its own network, just because doing so seems amusing and has few consequences.

The small size of this network and its highly localized nature obviously prohibit any claim of representativeness, but recent in-depth journalistic investigations of much more sophisticated and profitable hacker groups have uncovered similar patterns of distrust, hostility, and betrayal (Poulsen 2011, McCoy et al. 2012: 3, Olson 2012). Reports of these features, which are familiar to those who study more traditional types of criminal organizations (Von Lampe and Johansen 2004) or those who approach hackers from a psychological perspective (Schell et al. 2002), highlight the paucity of empirical research on hackers and reveal the need for criminology, sociology, and related disciplines to develop a more nuanced understanding of the social organization of malicious hackers. A core question to consider would be how skills and trust flow between such individuals when they are under external constraints such as law enforcement targeting, peer competition, and general market changes (Leeson and Coyne 2005). The criminal careers of offenders who straddle the line between street and online crime also promises to be a fascinating avenue of research. Such knowledge is important and is needed to offset the current public discourse on cybersecurity, which is too often characterized by hysterical statements about looming risks and presents hackers as a prodigious threat that requires extraordinary regulatory powers and the use of intrusive surveillance tools to preserve the internet from an impending state of anarchy. As seen in this chapter, malicious hackers are not exclusively beneficiaries of the chaos they create online – they can also easily fall victim to it, just like their street-offending counterparts.

References

ABU RAJAB, Moheeb; ZARFOSS, Jay; MONROSE, Fabian, and Andreas TERZIS (2006), “A multifaceted approach to understanding the botnet phenomenon”, *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, ACM: Rio de Janeiro, pp. 41-52.

ABU RAJAB, Moheeb; ZARFOSS, Jay; MONROSE, Fabian, and Andreas TERZIS (2007), “My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging”, *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*, ACM: New York, NY, pp. 1-8.

ANDERSON, Ross; BARTON, Chris; BÖHME, Rainer; CLAYTON, Richard; J.G. VAN EETEN, Michel; LEVI, Michael; MOORE, Tyler and Stefan SAVAGE (2012), “Measuring the cost of cybercrime”, *11th Annual Workshop on the Economics of Information Security*, DIW Berlin: Berlin, 25-26 June.

BÄCHER, Paul; HOLZ, Thorsten; KÖTTER, Markus and Georg WICHERSKI (2008), *Know your enemy: Tracking botnets – Using honeynets to learn more about Bots*, The Honeynet Project: Seattle, WA, available online at http://www.honeynet.org/book/export/html/50, last accessed July 25, 2012.

BARFORD, Paul and Vinod YEGNESWARAN (2007), “An inside look at botnets”, in Mihai CHRISTODORESCU, Somesh JHA, Douglas MAUGHAN, Dawn SONG and Cliff WANG (eds), *Malware detection*, Springer Verlag: New York, NY, pp. 171-191.

BORGATTI, Steve; EVERETT, Martin and Lin FREEMAN (2002), *Ucinet for Windows: Software for social network analysis*, Analytic Technologies: Harvard, MA.

BOYD, Danah and Kate CRAWFORD (2011), “Six provocations for big data”, *A decade in internet time: Symposium on the dynamics of the internet and society*, Oxford University: Oxford, 21-24 September.

CALCE, Michael and Craig SILVERMAN (2008), *Mafiaboy: How I cracked the Internet and why it is still broken*, Viking Canada: Toronto.

COLEMAN, Gabriella and Alex GOLUB (2008), “Hacker practice: Moral genre and the cultural articulation of liberalism”, *Anthropological Theory*, 8(3), pp. 255-277.

COPES, Heith and Lynne VIERAITIS (2008), *“Stealing identities: The risks, rewards and strategies of identity theft”*, in Megan MCNALLY and Graham NEWMAN (eds), *Perspectives on identity theft*, Criminal Justice Press: New York, NY, pp. 87-110.

DANCHEV, Dancho (2010), “Study finds the average price for renting a botnet”, *ZDNet*, 26 May, available online at http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528, last accessed on July 22, 2012.

DÉCARY-HÉTU, David and Benoit DUPONT (2012), “The social network of hackers”, *Global Crime*, DOI:10.1080/17440572.2012.702523.

FRANKLIN, Jason; PAXSON, Vern; PERRIG, Adrian and Stefan SAVAGE (2007), “An inquiry into the nature and causes of the wealth of internet miscreants”, *14th Conference of the ACM on Computer and Communications Security*, ACM: Alexandria, VA, 29 October-2 November.

FREEMAN, Linton; BORGATTI, Stephen and Douglas WHITE (1991), “Centrality in valued graphs: A measure of betweeness based on network flow”, *Social Networks*, 13(2), pp. 141-154.

GILMAN, Nils (2009), “Hacking goes pro”, *Engineering and Technology*, 4(3), pp. 26-29.

GRABOSKY, Peter (2007), “Editor’s introduction to special issue on transnational cybercrime”, *Crime, Law and Social Change*, 46(4-5), pp. 185-187.

GU, Guofei; PERDISCI, Roberto; ZHANG, Junjie and Wenkee LEE (2008), “BotMiner : Clustering analysis of network traffic for protocol- and structure-independent botnet detection”, *Proceedings of the 17th Conference on Security Symposium*, USENIX Association: San Jose, CA, pp. 139-154.

HERLEY, Cormac and Dinei FLORÊNCIO (2008), “A profitless endeavor: Phishing as tragedy of the commons”, *Proceedings of the 2008 Workshop on New Security Paradigms*, ACM: New York, NY, pp. 59-70.

HERLEY, Cormac and Dinei FLORÊNCIO (2009), “Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy”, *8th Workshop on the Economics of Security*, University College: London, 24-25 June.

HOBBS, Dick (1995), *Bad business: Professional crime in modern Britain*, Oxford University Press: Oxford.

HOLLINGER, Richard (1991), “Hackers: Computer heroes or electronic highwaymen?”, *Computers & Society*, 21(1), pp. 6-17.

HOLT, Thomas (2009), “Lone hacks or groups cracks: Examining the social organization of computer hackers”, in Frank SCHMALLEGER and Michael PITTARO (eds), *Crimes of the Internet*, Pearson: Upper Saddle River, NJ, pp. 336-355.

JORDAN, Tim and Paul TAYLOR (2008), "A sociology of hackers", *The Sociological Review*, 46(4), pp. 757-780.

KREBS, Brian (2011), "Rent-a-bot networks tied to TDSS botnet", *Krebs on Security*, 6 September, available online at http://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet, last accessed on July 22, 2012.

LAZER, David; PENTLAND, Alex; ADAMIC, Lara; ARAL, Sinan; BARABÁSI, Albert-Lázló; BREWER, Devon; CHRISTAKIS, Nicholas; CONTRACTOR, Noshir; FOWLER, James; GUTMANN, Myron; JEBARA, Tony; KING, Gary; MACY, Michael; ROY, Deb and Marshall VAN ALSTYNE (2009), "Computational social science", *Science*, 323(5915), pp. 721-723.

LEESON, Peter and Christopher COYNE (2005), "The economics of computer hacking", *Journal of Law, Economics and Policy*, 1(2), pp. 511-532.

LEMOS, Robert (2010), "Rise of the point-and-click botnet", *Technology Review*, 23 February, available online at http://www.technologyreview.com/news/417657/rise-of-the-point-and-click-botnet/, last accessed July 25, 2012.

LEYDEN, John (2011), "Bargain-basement botnet kit – yours for just €5", *The Register*, 22 September, available online at http://www.theregister.co.uk/2011/09/22/aldi_bot/, last accessed on July 22, 2012.

MCCOY, Damon; PITSILLIDIS, Andreas; JORDAN, Grant; WEAVER, Nicholas; KREIBICH, Christian; KREBS, Brian; VOELKER, Geoffrey; SAVAGE, Stefan and Kirill LEVCHENKO (2012), "PharmaLeaks: Understanding the business of online pharmaceutical affiliate programs", *21st USENIX Security Symposium*, USENIX: Bellevue, WA, 8-10 August.

MCCUSKER, Rob (2007), “Transnational organised cyber crime: Distinguishing threat from reality”, *Crime, Law and Social Change*, 46(4-5), pp. 257-273.

MEYER, Gordon (1989), *The social organization of the computer underground*, a thesis submitted to the Graduate School in partial fulfillment of the requirements for the degree Master of Arts, Criminology, Northern Illinois University: DeKalb, IL.

MITNICK, Kevin and William SIMON (2011), *Ghost in the wires: My adventures as the world’s most wanted hacker*, Little, Brown & Company: New York, NY.

MOORE, Tyler; CLAYTON, Richard and Ross ANDERSON (2009), “The economics of online crime”, *The Journal of Economic Perspectives*, 23(3), pp. 3-20.

MORSELLI, Carlo and Katia PETIT (2007), “Law-enforcement disruption of a drug importation network”, *Global Crime*, 8(2), pp. 109-130.

MORSELLI, Carlo (2009), *Inside criminal networks*, Springer: New York, NY.

MOTOYAMA, Marti; MCCOY, Damon; LEVCHENKO, Kirill, SAVAGE, Stefan and Geoffrey VOELKER (2011), “An analysis of underground forums”, *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement*, ACM: New York, NY, pp. 71-80.

NEWMAN, Graeme and Ronald CLARKE (2003), *Superhighway robbery: Preventing e-commerce crime*, Willan: Cullompton.

OHM, Paul (2008), “The myth of the superuser: Fear, risk and harm online”, *UC Davis Law Review*, 41(4), pp. 1327-1402.

OLLMANN, Gunter (2008), “Hacking as a service”, *Computer Fraud & Security*, 2008(12), pp. 12-15.

OLSON, Parmy (2012), *We are anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*, Little, Brown & Company: New York, NY.

PERLROTH, Nicole (2012), "Widespread virus proves Macs are no longer safe from hackers", *New York Times Bits Blog*, available online at http://bits.blogs.nytimes.com/2012/04/06/widespread-computer-virus-indicates-mac-users-no-longer-safe/, last accessed on July 4th, 2012.

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

REUTER, Peter (1983), *Disorganized crime: The economics of the visible hand*, MIT Press: Cambridge, MA.

ROGERS, Marcus (2006), "A two-dimensional circumplex approach to the development of a hacker taxonomy", *Digital investigation*, 3(2), pp. 97-102.

SCHELL, Bernadette; DODGE, John and Steve MOUTSATSOS (2002), *The hacking of America: Who's doing it, why and how*, Quorum Books: Westport, CT.

SHOVER, Neal (1996), *Great pretenders: Pursuits and careers of persistent thieves*, Westview Press: Boulder, CO.

STEVENS, Kevin and Don JACKSON (2010), *ZeuS banking Trojan report*, Secureworks: Atlanta, GA.

STONE-GROSS, Brett; COVA, Marco; CAVALLARO, Lorenzo; GILBERT, Bob; SZYDLOWSKI, Martin; KEMMERER, Richard; KRUEGEL, Chris and Giovanni VIGNA (2009), "Your botnet is my botnet: Analysis of a botnet takeover", in Somesh JHA and Angelos D. KEROMYTIS (eds.), *Proceedings of the 16th ACM Conference on Computer and Communication Security*, ACM: New York, NY, pp. 635-647.

TAYLOR, Paul (1999), *Hackers: Crime in the digital sublime*, Routledge: London.

TILLY, Charles (2005), *Trust and rule*, Cambridge: Cambridge University Press.

TREMBLAY, Pierre (1993), “Searching for suitable co-offenders”, in Ronald CLARKE and Marcus FELSON (eds.), *Routine activity and rational choice*, Transaction Publishers: New Brunswick, NJ, pp. 17-36.

TURGEMAN-GOLDSCHMIDT, Orly (2009), “The rethoric of hackers’ neutralizations”, in Frank SCHMALLEGER and Michael PITTARO (eds), *Crimes of the Internet*, Pearson: Upper Saddle River, NJ, pp. 317-335.

VON LAMPE, Klaus and Per Ole JOHANSEN (2004), “Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks”, *Global Crime*, 6(2), pp. 159-184.

WASSERMAN, Stanley and Katherine FAUST (1994), *Social network analysis: Methods and applications*, Cambridge University Press: Cambridge.

WERRY, Christopher (1996), “Linguistic and interactional features of Internet Relay Chat”, In Susan HERRING (ed.), *Computer-mediated communication: Linguistic, social and cross-cultural perspectives*, John Benjamins Publishing Company: Philadelphia, PA, pp. 47-63.

WRIGHT, Richard and Scott DECKER (1997), *Armed robbers in action*, Northeastern University Press: Boston, MA.

YAR, Majid (2005), “Computer hacking: Just another case of juvenile delinquency?”, *The Howard Journal*, 44(4), pp. 387-399.

YOUNG, Randall; ZHANG, Lixuan and Victor PRYBUTOK (2007), “Hacking into the mind of hackers”, *Information Systems Management*, 24(4), pp. 281-287.

ZARFOSS, Jay (2007), *A scalable architecture for persistent botnet tracking*, A thesis submitted in conformity with the requirements for the degree of Master of Science in Engineering, John Hopkins University: Baltimore, MD.

Table 1: Degree and flow betweeness centrality measures for the hacker network

	Degree centrality		Flow betweenness centrality	
	Degree	Share†	FlowBet (rank)	nFlowBet
1	85.000	0.376	32.401 (1)	45.001
378	50.000	0.221	8.160 (3)	11.333
516	24.000	0.106	9.219 (2)	12.805
134	20.000	0.088	2.551 (5)	3.543
564	18.000	0.080	1.267 (6)	1.759
286	13.000	0.058	8.140 (4)	11.306
142	8.000	0.035	0.120 (8)	0.167
121	6.000	0.027	0.000 (9)	0.000
841	2.000	0.009	0.936 (7)	1.300
737	0.000	0.000	0.000 (10)	0.000

Note: For valued data, non-normalized values are used (Borgatti et al. 2002).

†The share is the centrality measure of the actor divided by the sum of all the actor centralities in the network.

Table 2: Evolution of the distribution of high-trust, low-trust, and hostile relationships for network members

	2006			2007		
	Hostile (N)	Low trust (N)	High trust (N)	Hostile (N)	Low trust (N)	High trust (N)
121	0,0000	1,0000 (1)	0,0000	1,0000 (3) ↑	0,0000 ↓	0,0000
142	0,0000	1,0000 (2)	0,0000	1,0000 (3) ↑	0,0000 ↓	0,0000
841	0,0000	0,0000	1,0000 (2)	0,0000	0,0000	1,0000 (2) →
737	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
1	0,0000	0,7143 (5)	0,2857 (2)	0,2857 (2) ↑	0,4286 (3) ↓	0,2857 (2) →
286	0,0000	0,0000	1,0000 (5)	0,0000	0,0000	1,0000 (5) →
378	0,0000	0,6667 (4)	0,3333 (2)	0,1667 (1) ↑	0,5000 (3) ↓	0,3333 (2) →
134	0,0000	0,2500 (1)	0,7500 (3)	0,3333 (2) ↑	0,1667 (1)↓	0,5000 (3) ↓
516	0,0000	0,2000 (1)	0,8000 (4)	0,0000	0,2000 (1) →	0,8000 (4) →
564	0,0000	0,5000 (2)	0,5000 (2)	0,2000 (1) ↑	0,4000 (2) →	0,4000 (2) →
network	0,0000	0,4444 (16)	0,5556 (20)	0,2857 (12) ↑	0,2381 (10) ↓	0,4762 (20) ↓

Fig. 1: Valued ties within the hacker network. Thicker lines depict more frequent interactions

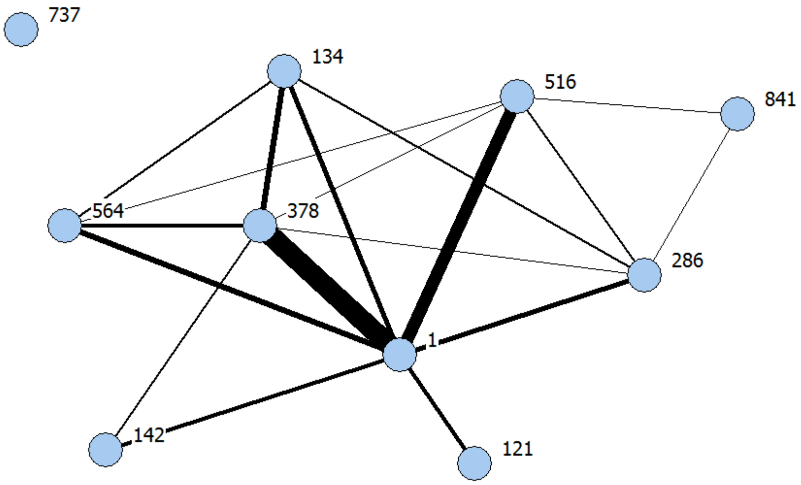


Fig. 2: Trust levels between network members in 2006. Solid lines indicate higher trust

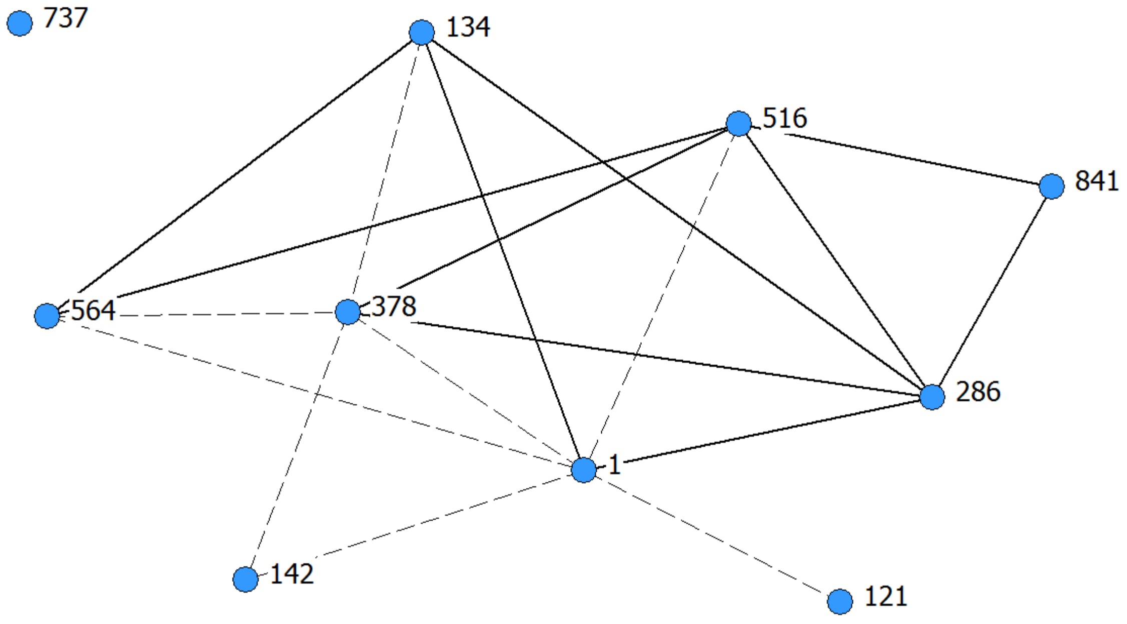
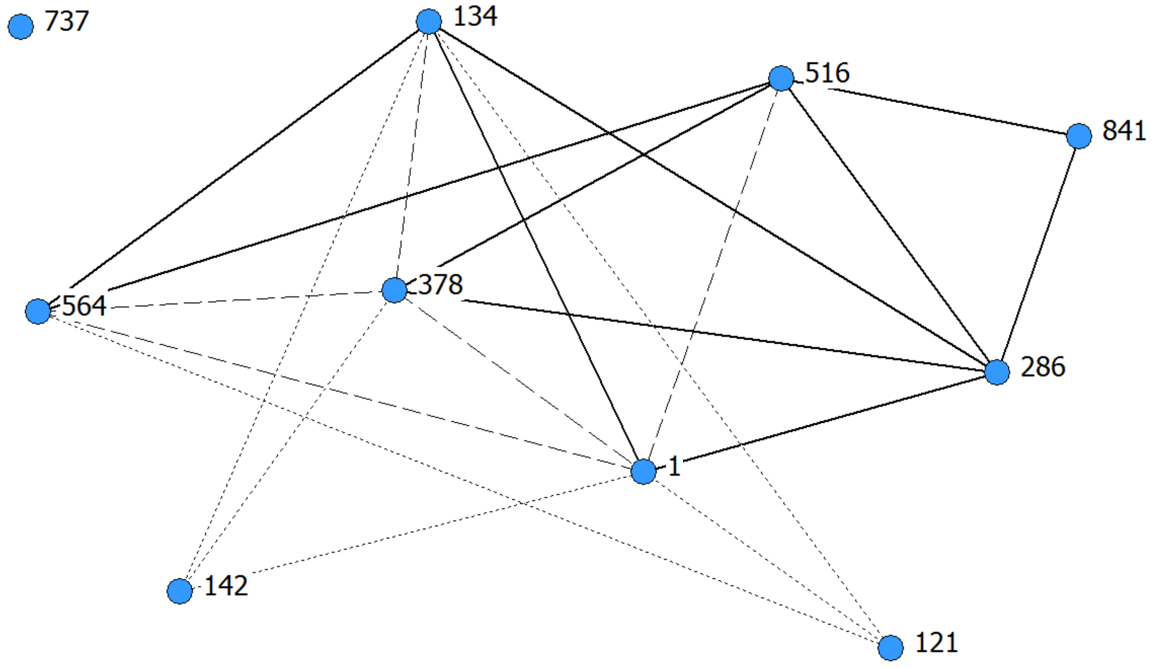


Fig. 3: Trust levels between network members in 2007.



___ higher trust

----- lower trust

……. hostility