Technical Report
TR-2010-004

"I'd Like to Pay with *Your* Visa Card" An Illustration of Illicit Online Trading Activity in the Underground Economy

Technical Report

Stefan Vömel[1], Thorsten Holz[2], and Felix C. Freiling[1]

[1] University of Mannheim, Germany
[2] Embedded Malware Workgroup, University of Bochum, Germany

Abstract. With the growing use and financial importance of the Internet, cyber criminals increasingly perceive computer systems, network architectures, and databases storing transaction- and personal-related data as assets and profitable targets. As illicit activities have become more organized and monetary-driven, a digital underground economy for hacking-related goods and services has evolved. In this paper, we outline the infrastructure and modes of operation of said economy with the help of real world samples captured in a communication channel on an IRC network. Thereby, we are able to gain a better understanding of the dynamics and interactions on this market.

1 Introduction

With an estimated number of 1.7 billion users and more than 206 million active sites, the Internet has evolved to one of the major information and communication platforms [16, 19]. With the growing acceptance of online trading and banking platforms, the commercial role of the World Wide Web has augmented as well: According to a recent Nielsen survey, 86% of the Internet population have ordered goods online at least once [20]. In the U.S. alone, retail sales in electronic commerce have climbed up to almost $127 billion [28]. The rapid economic growth has, however, also been accompanied by the evolution of a digital underground economy [6, 9, 27]. In special chat rooms and Internet forums, cyber criminals happily trade and abuse stolen credit card data, turning the once popular slogan "*I'd like to pay with my Visa card*" from a TV commercial in the 1990s into the opposite. Other transaction- and financially-related information such as login credentials for online bank accounts or shipping and delivery addresses containing personal data are frequently offered and requested as well. The extent of these activities has moved to a "point where it exceeds the capacity of a closed group" [6] and caught broad attention in both the popular and academic press more recently [6, 7, 9, 25–27].

1.1 Previous Work

A first insight into this economy was given by members of the Honeynet Project. By monitoring several communication channels on an IRC (*Internet Relay Chat*) network, they successfully discovered some type of automated credit card fraud [10]. Thomas and Martin analyzed the relationship between different market participants and tried to estimate the value of the economy [27]. The first extensive empirical study was presented by Franklin et al. [6]. With the help of machine learning algorithms, the authors categorized a data set of more than 13 million messages and identified a myriad of goods and services that are traded on the market. The results of a similar large-scale investigation were published by Symantec [25, 26]. In addition, various other researchers focused on special phenomena of the underground economy: Holz et al. attempted to assess the actual amount of the traded goods and services by examining captured keylogger data [9]. The physical and monetary effects of a spam network were observed by Kanich et al. [12]. Finally, Cova et al. investigated several identify theft-related toolkits that are offered in diverse channels of the IRC network [3].

1.2 Contributions

In accordance with prior work [6, 25, 32], we have monitored a branch of the underground economy over a period of 2 1/2 months and performed a brief quantitative evaluation. Our main focus, however, was to give a more *qualitative* description of this activity since the quantitative nature of previous studies usually leaves the behavior of the involved miscreants rather abstract to outsiders and non-security professionals. Therefore, we illustrate the interactions between the different participants on the basis of actual messages captured in the market. We feel that a presentation of real world examples can help develop a better understanding of the economy and perceive its participants as a community with their own interests, anxieties, and socio-cultural characteristics such as their own jargon and slang. Note that we have only analyzed market activity on an IRC network for this task. Other trading platforms of the underground economy such as online forums or malicious websites were not taken into consideration.

1.3 Outline of the Paper

The remainder of this paper is outlined as follows: In Section 2, we briefly illustrate the mode of operation of the IRC network that forms one of the bases of the underground economy. An overview of the data that we recorded in the course of the observation period in one IRC channel as well as our data acquisition technique is presented in Section 3, followed by a thorough description and analysis of the collected information in Section 4. The extent of the trading activity as well as particular characteristics of the market and its participants are shortly described in Section 5. We conclude with a summary of our findings and indicate opportunities for future work in Section 6.

2 Brief Background on IRC

The *Internet Relay Chat* (IRC) protocol provides a mechanism for real-time text communication over the Internet based on the client-server model [21]. Users typically log on to an IRC server with the help of a client application such as mIRC [17] or XChat [31]. Once a client has established a working connection, the user chooses a unique nickname (*nick*) for identification purposes and joins a so-called *channel* to start interacting with other participants. Messages can be either sent in the open and are broadcasted to all other channel members or be exchanged on a one-to-one basis in a private manner. In the latter case, the communication is not even accessible to the *channel operator*, a special user who possesses administrative and maintenance privileges, e.g., for specifying the topic of the discussion or removing (*kicking*) misbehaving users out of the channel. Many of these operations can be automated to a great extent and are frequently assigned to so-called bots [14], i.e., independently-running software programs. To enhance the security of a channel, operators may also define certain access rules. For instance, by setting a channel password (*keyword*) or making the channel invite-only, join operations can be easily restricted to a closed group.

3 Data Acquisition

3.1 Recording IRC Data with Compromised Honeypots

Over a period of about 10 weeks, from April 20, 2008 to June 30, 2008, we have monitored the channel `#ccpower` on the `Undernet` IRC network and recorded more than 676,000 messages. Access to the channel was obtained with the help of a compromised honeypot. A honeypot is "an information system resource whose value lies in unauthorized or illicit use of this resource" [23, 24] and is intentionally designed to be probed and attacked. Being bound to a number of network- as well as system-monitoring devices, a honeypot serves as an electronic bait and may help learn more about the behavior and characteristics of Internet miscreants [11, 22]. In our case, we were able to watch an adversary set up an IRC proxy (*bouncer*) and bot software on our system in order to take part in the trading activities of the underground economy. As the presence of the honeypot was not detected by the cyber criminal, all her actions as well as all public occurrences in the channel could be silently logged. We thus acted as a classic man-in-the-middle (MITM) between the system of the attacker and the IRC network (see Figure 1). More information about the approach can be found in the thesis by Vömel [29].

To date, a great part of the communication facilities of the underground economy can still be joined without difficulty [27]. However, current observation techniques are quickly rendered useless once miscreants start to limit access to a channel and cover their operations more carefully. In this case, a compromised honeypot may prove useful for maintaining an open door, assuming the presence of a monitored environment slips by the attacker. In the past, security professionals succeeded in disclosing covert actions with similar architectures [11, 22].

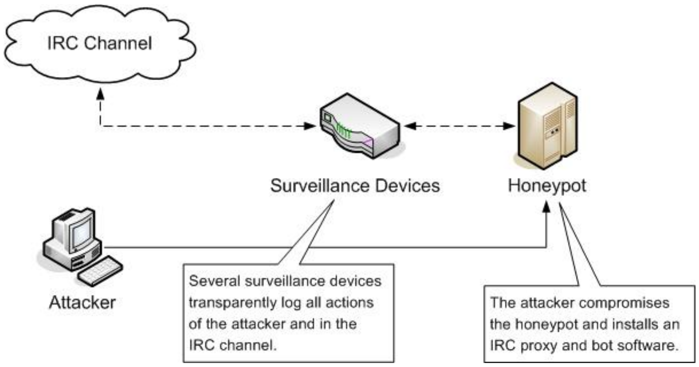
IRC Channel
Surveillance Devices
Honeypot
Attacker
Several surveillance devices transparently log all actions of the attacker and in the IRC channel.
The attacker compromises the honeypot and installs an IRC proxy and bot software.

Fig. 1: Setup of the Data Acquisition Architecture

3.2 Overview of the Collected Data

To a high degree, the recorded text corpora consisted of repetitively-sent messages. In many cases, automated scripts and programs periodically retransmitted pre-defined lines of text, for instance, advertisements for specific goods and services that are offered in the economy. For this reason, our data set of more than 676,000 collected messages could be reduced to a comparatively small working set of 4,165 unique posts, ordered according to their frequency. We manually categorized and labeled 10% (417) of the most frequent messages in the next step to accurately assess the recorded communication. Due to the characteristics of the frequency distribution, the labeled messages already covered 84.5% of the text corpora and were used as training data for a binary text classifier. Thereby, we were able to apply statistical machine learning techniques and automatically associate each of the more than 676,000 posts with a meaningful descriptor. Similar automatic text classification approaches were also used by several other authors in the past to process large quantities of captured IRC data [4, 6].

We outline the results of our research in the next section. Unless otherwise stated, our analysis is based on the labeled data.

4 Illustration of Illicit Activities in the Channel

All labeled messages were identified as either advertisements or requests for various cybercrime-related goods and services. The respective offers comprised about three quarters of the data set and outnumbered requests almost five to one. In addition, we assigned each message to one or more non-mutually distinctive categories in order to thoroughly classify the different data samples. In sum, we distinguished 10 categories as shown in Figure 2, namely offers and requests for (1) credit card-related data, (2) money transfer (*cash out*) operations, (3) hacked hosts, (4) online bank and (5) business accounts, (6) personal data, including addresses and phone numbers of the victims, (7) spam, (8) hacking, and phishing campaigns, (9) special hardware equipment that is required to carry out the operations, and finally, (10) so-called *confirmers* who act as intermediaries and verify the legitimacy of a business deal. We illustrate these categories in more detail in the following and present examples of real world messages that we have captured during the observation period.

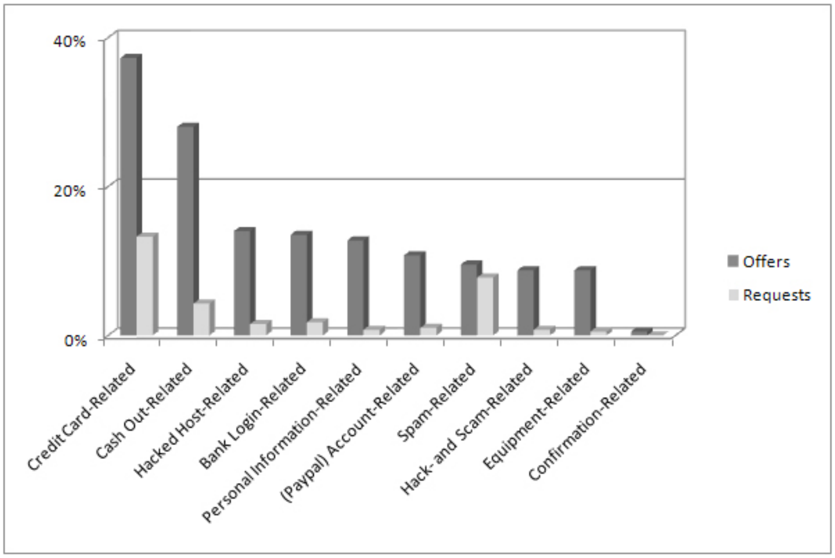

Fig. 2: Types of Hacking-Related Goods and Services

4.1 Credit Card-Related Offers and Requests

In almost 4 out of 10 cases, adversaries posted advertisements for stolen credit cards and credit card-related information. As McCarty [15, p. 91] points out, the data may either be obtained by breaking into computer systems and corporate databases or be physically provided by morally questionable personnel working at local banks, hotels, or restaurants (see also Line 7 of Listing 1).

Oftentimes, miscreants stated to possess both the personal identification number (PIN) of the victim as well as her card verification value (CVV2). The latter is a three-digit identification code that is frequently used for verifying the legitimacy of a credit card during online transactions. Some typical advertisements that we have captured during the observation period are shown in the upper half of Listing 1.

Prices for credit cards varied between $2 and $8 per piece. In many cases, the attackers also offered product bundles: In the example shown in Listing 1 (Line 13), 30 newly acquired ("fresh") cards ("CCz") were advertised for $200. Corresponding requests were found in only 13.25% of the data set. Several representative sample messages for this category are displayed in the lower half of Listing 1.

```
# Advertisements for Credit Cards and Credit Card-Related
# Information

"Selling valid fresh unused Mastercards/Visa/American
 Express (...)"

"Fresh Lists. Selling hacked admin shop & hotel database.
 DUMPS, FULLS, CVV2, TRACK2. 101 Skimmed only. (...)"

"SELLING SKIMMED DUMPS WITH PIN FROM GAS STATION!
 FOR BAD DUMPS; MONEY BACK AND REPLACE GUARANTEE! (...)"

"Selling Fresh France CCz With Cvv2 (...) 30ccz = 200$ (...)"

"Selling USA/Worldwide VISA/MC dumps from Bulgarian and
 Russian suppliers. Frum first hands! (...)"

"CVV2 FRESH IS HERE * * * 5,000 CVV2 FRESH IN HAND!
 200 FRESH DAILY! (...)"


# Requests for Credit Cards and Credit Card-Related
# Information

"Buying all valid cc's Visa or Mastercard 7$ Each ! (...)"

"MY BINLIST : http://<...>/bnss.txt - any card for 250$ !!!
 msg me if u have any !"

"I need cvv2 From Italy, Who have privat me (...)"

"NEED CVV2 SUPPLIER TO SUPPLY US AND NON US CVV AND WORK IN
 LONG TERM....PLS PM ME FOR GOD DEALZ YM:<...>@YAHOO.COM"
```

Listing 1: Sample Advertisements and Requests for Stolen Credit Cards and Credit Card-Related Information

4.2 Cash Out-Related Offers and Requests

One of the biggest challenges Internet miscreants face is to safely cash the illegally obtained funds while mitigating the risk of getting caught by law enforcement authorities at the same time [27]. For this reason, attackers frequently cooperate with so-called *cashiers*, i.e., brokers who are willing to clean out the bank accounts of the victims. For a pre-defined, fixed fee (e.g., 50% of the total amount) the cashier transfers the money directly to the adversary, typically within hours, by using online or offline services as offered by Western Union (WU) or E-Gold (see also Franklin et al. [6]).

Alternatively, the money may temporarily be moved to a *drop*, i.e., an intermediary domestic or offshore account, that helps impede prosecution and facilitates money laundering [27, p. 11-12]. In this case, so-called *confirmers* are frequently hired and act as trusted third parties to verify incoming payments. A list of selected advertisements and requests for cashiers, confirmers, and drops can be found in Listing 2.

4.3 Further Financial Account-Related Offers and Requests

In addition to credit cards, their corresponding PINs, and CVVs, several other types of financial account-related information were frequently offered and requested in the underground communication channel we observed. For instance, in 12.75% of all cases, adversaries advertised login credentials for various major national and international banks, e.g., HSBC, Halifax, the Bank of America (BOA), Chase, and Wells Fargo. Furthermore, attackers frequently offered access to numerous compromised online accounts, most importantly to *PayPal*, an electronic money transfer service, and *Amazon*, the world's leading Internet retailer [2]. On the other hand, with a share of 1.75% and 1%, respectively, corresponding requests for these goods and services were rarely posted (see Figure 2). Some sample messages for each category are illustrated in Listing 3.

4.4 Hacking-Related Offers and Requests

In almost one out of seven sample messages, adversaries offered compromised hosts for sale. These hosts may, for instance, serve as intermediaries for further attacks and, thus, impede prosecution [11]. Attackers also periodically advertised entire *botnets*, i.e., larger numbers of penetrated systems under control of the miscreant (see Listing 4, Line 6). In dependence of its size, a botnet may potentially cause severe havoc, e.g., by bringing down the network of a business competitor in the course of a *Distributed Denial of Service* (DDos) attack [18,22].

Compromised hosts may be used for *spamming* and *phishing* campaigns as well. In the latter case, an attacker first sets up a so-called *scam page* that mimics the web site of a legitimate, trusted service provider. In the next step, unaware computer users are lured into visiting the fraudulent page, typically by sending specially crafted email messages [30]. The victims are then tricked into entering their online credentials or other sensitive information that are particularly interesting for Internet miscreants. In 8.75% of the samples, adversaries explicitly advertised these types of services, the number of corresponding requests was, however, negligible. In contrast, offers and requests for spam-related operations were posted almost equally with a share of 9.5% and 7.75%, respectively. An overview of sample messages for this category is presented in Listing 4.

```
# Advertisements for Cashiers

"Cashout Usa / UK CC's Visa With SSN ONLY!
 50:50% Cashout in 2 hours,
 share in Wu / Egold / MoneyBookers PM ME FOR MORE"

"CASHING OUT MONEYBOOKERS ACCOUNT. (10.000$/DAILY)"

"I AM LEGIT CASHOUT OF ALL THESE BANK FROM $1 TO $50,000
 citibank,hsbc,natwest,lloyds,suntrust,boa, (...)"

"CASHING OUT DUMPS WITH PIN IN USA AT LOCAL ATM's
 PM ME FOR FAST CASHOUTS FOR YOU!!!!"

"Cashing Dumps + Pins / Fulls + Pins in 40 Mins
 Msg me For bins List!"

# Advertisements for Confirmers

"Confirm Western Union ...PRV ME"

"Got Western Union Bug [$265,$999.99]..
 It Can Confirm Automatically.."

"CONFIRM MTCN NUMBERS,MAKE WESTERN UNION ORDER"

# Advertisements for Drops

"I Got Legit U.S.A Item Drop, Split 50/50"

"Got drop for WESTERN UNION on UK LONDON (...) !!!"

"(...) THOSE WHO NEED INDIAN DROP FOR GOODS AND
 BANK LOGINS PLS PM ME"

"GOT WU DROP ON ANY NAME IN ROMANIA. SERIOUS BUSINESS (...)"

"HAVE CITI BANK KOREA AND CHINA DROPS
 THAT CAN TAKE UP $1,000,000 (...)"


# Requests for Cashiers, Confirmers, and Drops

"I am looking for someone in US that can cashout pins. (...)"

"SPAMMER looking for some deals/trustable casheers. !!!"

"I'm looking for a WU confirmer for long term business (...)"

"Looking for a USA/Canada Drop, USA/Canada CVV Cashier (...)"

"i need drops from uk (...) pm for deal"
```

Listing 2: Sample Advertisements and Requests for *Cashiers*, *Confirmers*, and *Drops*

```
# Advertisements for Bank Login and Online Accounts

"Selling Bank ACCOUNT !!!!
 big / small ballances US, UK, CA ONLY !!!"

"Selling (...) Bank logins with good balance (...)
 Contact msn: <...>@hotmail.com ICQ: <...>"

"i Got Few LLoyds Logins with 500 to 1800 Pounds,
 I dont want Cashiers I sell Them Only! Msg me For a Deal."

"Selling BOA for 20$ Hurry, Only Few to sell, Accept e-gold"

"I am selling a Verified Paypal account w/ full info! (...)
 here is a pic http://<...>/ppaccount.jpg - ICQ#: <...>"

"Selling (...) ShopAdmins,Paypalz,Amazons,(...) Accept WU!"

"Sells (...) Skype Accounts..Verified..
 Unverified PayPal Accounts With Mail Access..
 Ebay Accounts With Mail Access.."

"Selling steam accounts 5-6-7-8 digits, you tell me which
 game you want and I will get it for you. (...)
 If I don’t answer add me on msn: <...>@hotmail.com (...)"


# Requests for Bank Logins and Online Accounts

"(T)rade for PayPal and some bank logins - (...) icq <xxx>"

"I am Looking For Paypal Supplier, I can Cash 220 $ from
 each verified Paypal Account (...) I’ll send your share
 with in 2-3 Hours via e-gold or Western Union (...)"

"I NEED PAYPALS ACCOUNTS!!! I HAVE BANK LOGIN AND FULLZ!!!"

"BUYING ALL VERFIED PAYPALS E-GOLD/WEST UNION"

"I need Any Company Account in USA, If you have PM me! (...)"
```

Listing 3: Sample Advertisements and Requests for Bank Logins and Online Accounts

```
# Advertisements for Hacked Hosts, Spamming Campaigns,
# and Scams

"(S)elling hacked roots:linux,freeBSD, sunOS; (...)"

"Selling botnets/bots For Reasonable Prices (...)"

"Selling Socks of All Countries with Great UpTime. (...)
 1 SOCK = 1$, Buy 3 Get 1 For Free (...)!"

"SELL Root's, Shells[c99/r57], RDP's, VNC's, Socks5/Proxy's,
 Cpanels, Inbox Mailer, Priv8 RFI Scanner! E-Gold Accepted!"

"Selling (...) Hacking & Injection Tool's and Scanners (...)
 TEACHING HACKING CLASS! Trades and Deals Welcome!"

"Has Scamms , Hacked hosts , Mails , SSH Scanner , (...)
 I make Scams upon Request (...)"


# Requests for Hacked Hosts, Spamming Campaigns, and Scams

"I want to buy root`s or remote desktop
 msg me payment via e-gold"

"NEED REMOTE FROM USA - (...) TRADE FOR ROOT URGENT !"

"Selling Fresh 5Million Email List For Spamming"

"i need parmanent spamming host ...i pay egold"

"I AM NEED OF A GOOD HACKER THAT CAN SPAM AND AS WELL DEAL IN
 OTHER AREA, ANYBODY HERE THAT HAVE AN INBOX PHP MAILER AND I
 WILL TRADE WITH 10FFULLZ"

"I need Scam Page Designer !! Msg me now !!"
```

Listing 4: Sample Advertisements and Requests for Hacked Hosts, Spamming Campaigns, and Scams

4.5 Personal Information-Related Offers and Requests

As a supplement to credit cards, miscreants also frequently advertised so-called *fulls*, i.e., records of personal data that include the full address of the cardholder, her phone number as well as her email address. This information may help miscreants to impersonate (*steal*) the identity of a victim (see the third example in Listing 5, Line 7, and McCarty [15]). Samples as the one shown in Listing 6 were periodically posted to the channel, possibly to stimulate demand or prove data possession (see also Thomas and Martin [27]). In sum, we identified 12.75% of the labeled data as advertisements for this category. Surprisingly, however, this type of asset was requested in less than 1% of all cases.

```
# Advertisements for Personal Data

"Sell Fresh Full Info & Cvv2 (AU,CA,UK,US,IT,SP,EU) (...)"

"Selling (...) Fullz Info -> 20$ each [ICQ for DEAL: <...>]"

"SELLING CANADIAN ID'S, Be anyone you WANT! (...)"

"SELLING..US-CA-UK FRESH Fulls MMN/SSN/PIN/DOB (...)"


# Requests for Personal Data

"Need Valid US Cvv2 & Full info (...) Msg.me Ready to Deal
 A.S.A.P!!!"

"need ssn/dob, Full info! Paying 100$ via egold,paypal,
 or wu."

"I am interested in buying USA bank logins and FULLZ.
 Any legit seller should msg me pronto. Rippers stay off!!"

"BUYING CC FULLZ!  WILL BUY 10 FIRST SHOT,
 IF SATISFIED, WILL BUY MORE"
```

Listing 5: Sample Advertisements and Requests for Personal Data

```
Credit Card Number: 52xxxx1733xxxx3x
CVV:                761
Expiry Date:        06/10
Name:               Eurie <...>
Address:            <...> Ave Apt 3
ZIP:                <...>
State:              Texas
Country:            United States
Phone Number:       <...>
Email Address:      <...>@msn.com
```

Listing 6: Sanitized Example of a Full Personal Record

4.6 Equipment-Related Offers and Requests

The hardware equipment which is needed to retrieve credit card-related information was also offered for sale in the monitored communication channel. In particular, attackers advertised so-called *skimmers* as well as cameras for automated teller machines (ATMs). With these devices, miscreants are able to secretly record the PIN number as well as the respective carding data when a victim withdraws money from her account. The latter may then be processed by a MSR-206 magnetic card writer to create a new, valid duplicate. Prices for such a machine varied between $400 and $600 in the channel. Five typical product advertisements and a request that we have been confronted with in the channel are shown in Listing 7.

```
# Advertisements for Hardware Equipment

"Selling ATM SKIMMER FULL PACKAGE , included + MSR206
 ( with all accessories) , video available (...)"

"Selling ATM SKIMMER + MSR206 with
 5 blank magnetic cards (...)"

"ATM Skimmers, Cameras, MSR206, Readers, etc. for sale (...)"

"Selling MSR-206 for 600 USD dollars shipped to anywhere
 in the world. PM ME IF NEEDED."

"Selling (...) ATM Skimmers (S1) with Wireless Camera or
 PinPad with rechargeable battery 120hrs (...)"

# Request for Hardware Equipment

"LOOKING FOR MSR 206 /MSG FOR MORE INFO."
```

Listing 7: Sample Advertisements and Requests for Hardware Equipment

5 Market Activity and Market Characteristics

In the course of the observation period, we registered a total of 1,345 different users, as distinguished by their unique nickname. On an average day, 49 users were simultaneously logged on and posted at least one message to the channel. The market was affected by a high fluctuation though: 64.54% of the users left the channel within 24 hours (see Figure 3). After 7 days, less than 5% of the participants were still taking part in the actions. A possible reason for this behavior may, for instance, be that a majority of users either completed their transactions within a short amount of time or quickly left the channel because their expectations were not sufficiently met, or alternative channels were more promising. On the other hand, a small core of 36 members remained active for 10 days or more, e.g., to intensify business relationships with other Internet miscreants and maximize their profit margins in the long term (see also Franklin et al. [6]).

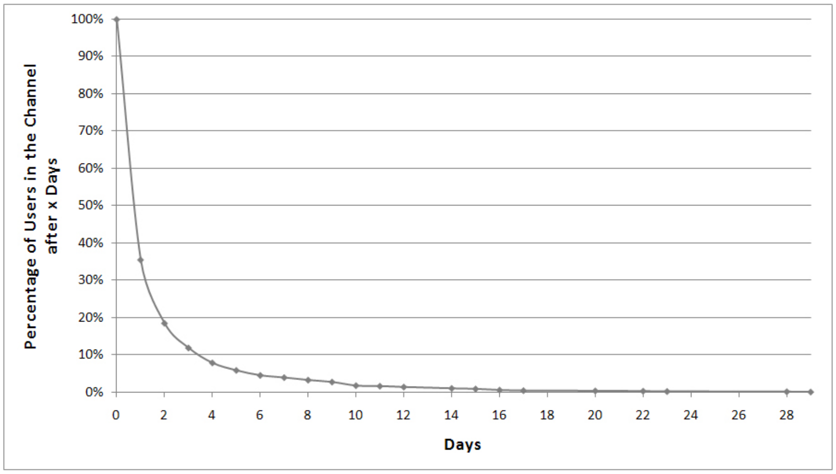

Fig. 3: Percentage of Remaining Users in the Channel after x Days

Apart from the high fluctuation, other prevailing characteristics of the underground market we observed were a high level of uncertainty and, what Franklin et al. call a “culture of dishonesty and distrust” [6]: Many participants appeared to be constantly concerned about “getting ripped”, i.e., being conned by other channel members (see Listing 8). In case a fraudulent operation was detected, the victim frequently posted a warning message for other users to the channel (see the last third of Listing 8), and the “ripper” was excluded from the market. Similar observations were also reported by Thomas and Martin [27]. Franklin et al. note, however, that these warning messages can also be used *against* the underground community to see a “marked decrease in the number of successful transactions” [6, p. 13]: By defaming and accusing regular sellers of dishonesty, their respective status can be systematically eliminated. Thereby, quality sellers increasingly lose their customer base, are unable to maintain their price level, and are finally forced to cease their trading activity. In the long term, a *lemon market* situation is created, i.e., buyers cannot reliably distinguish the quality of goods and services any longer due to a high degree of uncertainty [8]. As a consequence, the economy eventually collapses [1]. As Franklin et al. conclude, this is “a desired outcome” [6, p. 13].

```
# Sample Messages from Sellers

"HAVE VIRGIN USA SKIMMED DUMPS FOR SHOPPING (...)
 RIPPERS DON'T WASTE MY TIME!
 CONTACT ME ONLY IF YOU'RE FOR REAL."

"CASHING CANADIAN DUMPS, 50/50 Share,
 No Rippers! Serious People Only!"

"Selling EU dumps with pin [track1/track2] (...)
 NO KIDS,NO TESTS,NO RIPPERS....
 IF YOU WASTE MY TIME I WILL IGNORE YOU!!! (...)"

"I Got Legit U.S.A Item Drop,....Split 50/50 (...)
 Serious Drops for Serious Carders.
 NoOoOo Bull$hit ,Haters, Lamers or Rippers!!!!! (...)"


# Sample Messages from Buyers

"SPUNKY_DOG is  a ripper  stay away from him"

"SPANISHFLY is a ripper don't trade with him!"

"J0nah and Junkcode, are two ripper, be carefull (...)"

"LeeDevil is ripper avoid him"
```

Listing 8: Sample Messages Indicating Distrust in Other Market Participants

6 Summary and Future Work

We have monitored a communication channel on an IRC network that was used for illicit trading activities of stolen credit cards and other transaction- and personal-related data. We illustrated the different goods and services that are offered and requested in this branch of the underground economy based on a number of real world samples. In addition, we outlined major noticeable characteristics of the market and its participants. Our aim was to provide an *illustration* of this activity, i.e., a more qualitative description than previous quantitative studies have given.

To date, research has mainly focused on analyzing the advertisements and requests for the specific goods and services of the economy. However, there still seems to be some disagreement about the extent and profitability of the market. For instance, Symantec estimates the total value of advertised goods to be higher than $276 million [25]. In contrast, Franklin et al. report a considerably lower estimated value of about $93 million [6]. Herley and Florêncio doubt the correctness of both values and criticize that "there is not a single confirmed instance of a sale of illicit goods" documented in previous studies [8, p. 9]. As authors had lacked to specify the rate of business deals that are actually closing, "[o]ne cannot estimate the gold in the mountains from the activity at the shovel store". We share this opinion and believe that market activity is a poor indicator for the wealth of the economy, thus, other techniques for studying the underground economy are necessary.

To impede illicit market transaction, several theories have been discussed but have not been implemented yet: Franklin et al. propose two simple and elegant counter-measures based on deceptive accounts and false defamation (see Section 5 and Franklin et al. [6]). Ford and Gordon as well as Li et al. present two approaches to raise the level of uncertainty in malicious botnets, making these activities economically unviable [5, 13]. Similar mechanisms may certainly be applied to other structures of the underground market, too.

Last but not least, data acquisition techniques must be adapted to cope with access-restricted channels, too. We have suggested the use of compromised honeypots as a potential means of gaining access in this situation. Whether this solution is methodologically sound to systematically infiltrate covert trading platforms still needs to be examined in more detail in the future though. Thus, as the arms race continues, the underground market will remain fascinating and interesting to observe.

References

1. Akerlof, G.A.: The market for "Lemons": Quality uncertainty and the market mechanism. The Quarterly Journal of Economics 84(3), 488–500 (1970)
2. Brohan, M.: The top 500 guide (June 2009), http://www.internetretailer.com/article.asp?id=30594
3. Cova, M., Kruegel, C., Vigna, G.: There is no free phish: An analysis of "free" and live phishing kits. In: Proceedings of the 2nd Conference on USENIX Workshop on Offensive Technologies (2008)
4. Elnahrawy, E.M.: Log-based chat room monitoring using text categorization: A comparative study. In: Proceedings of the International Conference on Information and Knowledge Sharing (2002)
5. Ford, R., Gordon, S.: Cent, five cent, ten cent, dollar: Hitting botnets where it really hurts. In: Proceedings of the 2006 Workshop on New Security Paradigms (2006)
6. Franklin, J., Paxson, V.: An inquiry into the nature and causes of the wealth of internet miscreants. In: Proceedings of the 14th ACM Conference on Computer and Communications Security (2007)
7. Goldman, D.: Cybercrime: A secret underground economy (September 2009), http://money.cnn.com/2009/09/16/technology/cybercrime/index.htm?postversion=2009091613
8. Herley, C., Florêncio, D.: Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In: Proceedings of the Workshop on the Economics of Information Security (WEIS) (2009)
9. Holz, T., Engelberth, M., Freiling, F.: Learning more about the underground economy: A case-study of keyloggers and dropzones. In: European Symposium on Research in Computer Security (ESORICS) (2009)

10. Honeynet Project: Know your enemy: A profile (June 2003), http://old.honeynet.org/papers/profiles/cc-fraud.pdf
11. Honeynet Project (ed.): Know your Enemy - Learning about Security Threats. Addison Wesley (2004)
12. Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M., Paxson, V., Savage, S.: Spamalytics: An empirical analysis of spam marketing conversion. Communications of the ACM 52(9), 99–107 (2009)
13. Li, Z., Liao, Q., Striegel, A.: Botnet economics: Uncertainty matters. In: Proceedings of the Workshop on the Economics of Information Security (WEIS) 2008 (2008)
14. Lo, J., Campling, A.: The new irc channel operator's guide (August 2008), http://irchelp.org/irchelp/changuide.html
15. McCarty, B.: Automated identity theft. IEEE Security & Privacy 1(5), 89–92 (2003)
16. Miniwatts Marketing Group: World internet users and population stats (September 2009), http://www.internetworldstats.com/stats.htm
17. mIRC Co. Ltd.: mirc: Internet relay chat cient (2010), http://www.mirc.com/, http://www.mirc.com/
18. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review 34(2), 39–53 (2004)
19. Netcraft: January 2010 web server survey (January 2010), http://news.netcraft.com/archives/2010/01/07/january_2010_web_server_survey.html
20. Nielsen Company: Trends in online shopping (February 2008), http://th.nielsen.com/site/documents/GlobalOnlineShoppingReportFeb08.pdf
21. Oikarinen, J., Reed, D.: RFC1459 - Internet Relay Chat Protocol (May 1993), http://www.faqs.org/rfcs/rfc1459.html
22. Provos, N., Holz, T.: Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison Wesley (2007)
23. Spitzner, L.: Definitions and value of honeypots (May 2003), http://www.spitzner.net/honeypots.html
24. Spitzner, L.: Moving forward with defintion of honeypots (May 2003), http://www.securityfocus.com/archive/119/321957/30/0/threaded
25. Symantec: Symantec report on the underground economy (November 2008)
26. Symantec: Symantec global internet security threat report (April 2009), http://www4.symantec.com/Vrt/wl?tu_id=gCGG123913789453640802
27. Thomas, R., Martin, J.: The underground economy: Priceless. The USENIX Magazine 31(6), 7–16 (2006)
28. U.S. Census Bureau: 2007 e-commerce multi-sector e-stats report (May 2009), http://www.census.gov/econ/estats/2007/2007reportfinal.pdf
29. Vömel, S.: Using Honeypots to Capture and Analyze Malicious Activities on the Internet. Diploma thesis, University of Mannheim (August 2009)
30. Watson, D., Holz, T., Mueller, S.: Know your enemy: Phishing (May 2005), http://www.honeynet.org/papers/phishing/
31. Zelezny, P.: Xchat - windows & linux chat program (2009), http://xchat.org/
32. Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., Zou, W.: Studying malicious websites and the underground economy on the chinese web. In: Proceedings of the Workshop on the Economics of Information Security (WEIS) 2008 (May 2008)