CASHING 0ut

Exploring Underground Economies

Kurt Thomas
kathoma2@uiuc.edu

David Albrecht
dalbrech@uiuc.edu

Abstract

Underground economies by nature defy their very name. Publicly advertised, these illicit digital markets operate with little concern for law enforcement or retaliation, offering a meeting ground for the internet savvy and technically challenged alike to buy and sell stolen credit card information and identities. By examining the multitude of underground markets in operation it is possible to categorize the roles of the individuals partaking in illicit trades as well as identify the types of data being sold and the mediums exercised to make payments and extract funds from stolen credit cards. The sheer volume of traffic that populates these markets leads us to question how digital fraud can be combatted and what information can be garnered by monitoring underground economies.

Keywords: free cc plz, carders, cashout, cvv2, egold, lolz, underground economies, identity theft, internet fraud.

1 Introduction

Identity theft presents a rising challenge to digital security. The United States Federal Trade Commission recently reported that up to 9 million Americans could become victims of identity theft each year [1]. Current trends towards large-scale customer data aggregation exasperate the threat of compromise as even isolated break-ins at data centers can have devastating effects (see [2], involving theft of over 40 million cards).

The culprits of identity theft are not the highly sophisticated or the shadowed elite. The anonymity of the internet and the ease of communication has given rise to underground markets, digital market places where parties engage in commercial transactions to monetize stolen identities. In these marketplaces, a multitude of participants provide varying services. Credit data and identities can be bought and sold, aid in dumping accounts can be enlisted, and bank insiders can be tapped to help launder funds. Despite the term "underground", these markets operate in the complete open, actively advertising to new members who can provide services or potential buyers.

Our work follows on the heals of previous exploration conducted by [3, 4] amongst others. Building on their findings, we accessed and logged several markets that operated via IRC channels and bulletin boards in the hopes of finding new trends and providing a better classification of the individuals involved in the underground economy. In Section 2 we detail the types of market participants, continued on in Section 3 with the actual data and services for sale. Section 4 addresses the issues of trust that burden underground economies and the risk of fraud by market participants. Section 5 follows with an explanation of how criminals of the underground are laundering funds and who really bares the cost of identity fraud. Section 6 examines the technical sophistication of users and their ability to circumvent law enforcement, while finally Section 7 addresses the possibility of defeating the underground economy and what protections can be emplaced to curb the rising threat of identity theft. It is our hope that by examining these issues and monitoring underground marketplaces, security researchers can identity trends in the underground market and identity the primary sources of identity theft, ultimately leading to better protections to be constructed.

2 Naming the Players

Underground economies are not limited to the digital elite. Markets boast the membership of bank employees who launder funds, business employees willing to provide stolen credit data, and global shipping addresses which act as intermediary drop points before goods are forwarded on to their final destination, all of these actions building on a reputation system to guard against scams. Comprehending the vast number of participants taking part in the sale of illicit data is best motivated by an example transaction that could

be witnessed on any day-to-day operation.

Pretend for a moment Eris is an up and coming credit card thief who's become aware of underground markets by means of mainstream media and the barrage of headlines covering credit card fraud and identity theft [5, 6]. Armed with only a basic knowledge of what these markets sell, she hits up her favorite search engine and types away the terms the media most often advertised:

```
<search> buy cvv2, carder, forum </search>
```

With minimal effort, Eris discovers a multitude of internet forums advertising places to buy and sell stolen credit card information. Eris sees an advertisement for a rival marketplace that uses an internet chat relay (IRC) and hops on a channel `#cc-trades`, user name `Eris<3ccv2`. Within moments of joining Eris is bombarded with advertisements by automated bots purporting to sell credit cards for as low as $2 for accounts with limits exceeding $1,000, full identities, bank logins, and a multitude of other goods. With little concern for being scammed, Eris contacts one of these sellers (`Stranger7`) in private and strikes up a deal. Via paypal, she'll transfer $20 for ten credit cards along with each cards entire identity; name, address, card number, and verification number - everything necessary to complete a digital transaction. Stranger7 gives his paypal account information and Eris sends him the demanded fee, shortly after which Eris receives data pertaining to ten individuals' credit cards.

Eris, aware of the threat of being caught by the federal government, decides against simply purchasing a new LCD wide-screen TV and sending it to her house. She needs some way to liquidate her newly bought credit cards that can't be linked back to her. Just her luck, the advertisements continue to spew over the IRC channel. Need to cash out accounts? There are people to help. A number of competing advertisements purport abilities to cash out accounts directly from the bank or to act as a forwarding address for Eris' desired TV. Simply reading over the offers, Eris can elect her method of choice for obtaining 'her' money.

It's just another day in the world of underground markets.

Whether this story is believable or not, underground markets exist and their participants are more than willing to hawk their goods and services. From the variety of advertisements that appear on carding forums and IRC channels, participants can be categorized into a number of roles: *buyers, carders, cashiers, drops, rippers, and operators.*

2.1 Buyers

A *buyer* is any individual looking to purchase goods or services provided by other members of the underground market. Want-ads are posted to IRC channels and forums manually or through the use of automated bots while actual purchases happen in private messages via IRC, e-mail, or instant messaging clients.

Examples:

```
<buyer a> need fresh US Fullz Msg Me Fast If
U have Am Payin E-gold.
<buyer b> i buy uk cc's ..prv me only serios
ppl 4 good dill.
<buyer c> Looking to buy HSBC debit with pins
and CC's.....
```

2.2 Carders

The backbone of underground markets hinges on *carders* supplying stolen credit card and identity information for a fee. These individuals will advertise their inventory of stolen data ranging from credit cards with the necessary authentication information to full identities including driver's license numbers and social security numbers. Often included in these advertisements are details pertaining to pricing information and the carder's preferred method of payment.

Examples:

```
<carder a> selling US (Visa, Master) $2, UK
(Barclay) $3.  e-gold only
<carder b> selling us, uk fresh fulls (master
& visa) $10.  I accept paypal or e-gold
<carder c> Am Selling US, UK Mastercard,
Visa, and American Express Fulls, Fresh and
100% valid, WIth DOB, SSN, DL.
```

2.3 Cashiers

Once a buyer purchases a credit card he needs some method of dumping the account's funds. The methods of "cashing out" will be detailed later in Section 5, but certain market participants will advertise their ability as *cashiers* to dump the entire contents of an account. The most advertised method of laundering money is via Western Union where a cashier will pose as the initiator of a money order (required to be in the country of origin of the stolen credit card) with the recipient being either another cashier

or the buyer. Other individuals are bank employees who have some semblance of reputation with the bank and can transfer funds from one account to another. The typical fee for such services range from a 50-50 split or 70-30 with the cashier taking 30%.

Examples:

```
<cashier a> i Cash Out Wells fargo, Boa,
Nation Wide, Chase, WachoviA, WaMu, Citibank,
Halifax Msg me.
<cashier b> I Cashout Skimmed Dumps + Pins
30/70 % Split i Take 30% You Take 70%.
<cashier c> can cashout cvv's via WU terminal
agent.  500-700 $ per cvv's pvt me for more
info.
```

2.4 Drops

An alternative to a cashier is a *drop*, an individual who acts as a forwarding address for illegally purchased goods. Rather than risk ones home address when purchasing a new laptop online, a buyer can use a drop as an intermediary address before goods are forwarded on to the buyer. For parties residing in countries that businesses will not ship to, drops provide a method to circumvent export policies.

Examples:

```
<drop a> i drop in usa i can pick any name.
<user b> F@!k drops man, I ship to my friends
house, no fee.
<user c> u will lose ur friends soon!  ^^
<user d> I guess some friends are expendable!
```

2.5 Rippers

Despite the simple means of profiting from legitimate transactions, even underground markets are plagued by the threat of criminals. *Rippers* are market participants who try to scam other members into buying non-existent goods or fail to fulfill their end of bargains. While there are no obvious signs that pin a participant as a ripper, deals that seem too good to be true provide some insight into high-risk transactions.

Examples:

```
<ripper> Selling software to verify your
cvv2.  Great for carders, payment is $10.
<ripper> Selling database of 350,000 cvv2!
msg me fast for good deal!!!
```

2.6 Operators

In order to curb the practice of scamming, underground markets have adopted a reputation system where sellers can achieve *verified* status as a badge of honor their services are legitimate. *Operators* are typically channel or forum owners who act as a root of trust and check into the credibility of potential sellers. The process of achieving verified status differs from market to market, but typical methods require a monetary fee along side free samples of valid credit cards (or the service being provided) that can be tested. Community members also report successful or unsuccessful purchases to help build or destroy a seller's reputation. Verified sellers are marked in forums with specially colored titles ('gold status') where as in IRC they receive the voice attribute (+v) which is publicly noticeable. The same market operators can ban participants due to reports of scamming or can remove a participant's verified status.

While achieving verified status says nothing about the actual quality of the seller outside the market operator's opinion (and in some cases the community's opinion), it's within the interest of the operator to be associated with legitimate sellers in order to build their own market presence and reputation, reaping further reward from new members looking to become verified.

Examples:

```
<@operator a> If you want verified status msg
me, cost is $50.
<@operator b> To become verified pm any @op.
```

3 Sale! Sale! Sale!

Whether invoking an image of a back street bazaar or a highly systematized marketplace, competing underground economies all offer the same data and services for sale. By examining advertisements and interpreting the disparaging language of questionable English, acronyms, and market-speech, a classification of advertisements appears that underground economies have adopted as a *modus operandi*. The break down of products includes credit cards, full identities, bank logins, technical services, and otherwise common goods.

3.1 Basic Credit Data: CVV2s

The most pervasive products available in underground markets are stolen credit card numbers along with the card owner's billing information and associated credit validation value (CVV2). Sellers will advertise

the card's country of origin and sometimes the card provider (Visa, Mastercard, etc). Advertisements we encountered offered "cvv2 cards" at a rate of $2 to $3 from verified market members for cards from almost any country in the world.

Example Advert:

```
<seller> I sell US, UK cvv2 Normal info (CC
number+exp+cvv2, Cardholder, billing addrs).
Msg me!.
<seller> I Got, US, Uk, MX, IT, AU, RU,
Chille, CA Cvv2
```

Sample CVV2:

```
Name:  Paul Drensen
Street:  439 Main St
Postcode:  61801
City:  Urbana
State:  Illinois
Country:  United States
CC Owner:  Paul Drensen
CC Number:  4417123142102878
CVV2:  912
Date Expire:  03/08
Telephone:  (217) 332-3921
Email:  paul_drensen@gmail.com
```

3.2 Full Identity Data: Fullz

The next step up from buying a cvv2 is to buy an individuals entire identity. "Fullz", as they are referred to, range in the data set available, but typically include an individuals credit information in addition to their social security number and date of birth. Depending upon the advertisement, some fullz offer mother's maiden name, drivers license number, or even a passport number. The typical asking price of a full ranged between $10 and $25.

Example Advert:

```
<seller> US fullz cvv2 (CC number+exp+cvv2,
Cardholder, billing address, DOB, SSN, MMN,
Passport number).
<seller> Got Uk FuLLs each 15$, US FULLs each
10$.
```

Sample Full:

```
Name:  Paul Drensen
Street:  439 Main St
Postcode:  61801
City:  Urbana
State:  Illinois
Country:  United States
CC Owner:  Paul Drensen
CC Number:  4417123142102878
CVV2:  912
Date Expire:  03/08
Telephone:  (217) 332-3921
SSN: 325-72-2234
Date of Birth:  07/19/1964
MMN: Steingard
Email:  paul_drensen@gmail.com
```

3.3 Bank Logins

The alternative to buying card information is to buy a stolen bank login. The banks most commonly advertised included Bank of America (BoA), Wells Fargo, Washington Mutual (WaMu), Chase, and Wachovia. To support the promise of high balance accounts advertisements often include the seller's willingness to provide screen shots of the login's account summary.

Example Advert:

```
<seller> Got US Chase Logins with high
balance sell 300$
<seller> I have Wells + BoA + WaMu login, msg
me, e-gold only
```

3.4 Services

In addition to buying and selling stolen credit identities, channels are often visited by advertisements for country-centric mailing lists, rooted servers, re-mailers, socks proxies, and botnet access – all from the same seller. Pricing data for such services was not readily available from IRC channels and forum advertisements for similar goods typically asked interested buyers to contact the seller directly for pricing information.

Example Advert:

```
<seller> selling hacked host (cpanel
| ftp account | c99 and r75 shell
uploaded & injected) inbox mailer ||
Hacked root(ssh protocol) || fresh
maillist us/ca/fr/uk/de/au/ksa/it ...
(yahoo/aol/hotmail...  or mixed) || bot vuln
scan || exploit || and more hacking stuff ||
egold Only
```

3.5 Other

Included here for completeness, other prevalent advertisements included stolen eBay and PayPal logins.

4 Treachery: Issues of Trust

Carders, cashiers, drops, the promise of full identities, and quick payment; the underground economy has much to offer, but is any of it true? The common e-mail box today is bombarded with fraudulent advertisements, scams, and click-on ads to make $1,000,000 dollars and the underground is no less susceptible. Rippers, the cordial term for scammers of the underground, prey on the gullible, the unsuspecting, and even seasoned participants. The inherent anonymity of purchases and lack of enforcement to deter rippers leaves markets susceptible to issues of trust. While verified participants carry some reputation, that reputation is entirely dependent on the reports of other community members and the honesty of market operators.

4.1 Market Believability

Paranoia should raise the issue then if anyone can be trusted. Why should carders with access to hundreds of credit card numbers sell them for $2 rather than cash them out for far greater returns? Why should a drop be trusted to forward a package on rather than keep it? Insight into the credibility of markets requires knowledge of how often sales are conducted and whether they go wrong. As communication for purchases is conducted in private, simply monitoring IRC channels and forums will not evince any knowledge of market activity. However, the existence of forums and operators to report deals gone wrong allows some insight that participants are trying to make purchases. Likewise, when free credit cards are posted and instantaneous feedback appears of `card was valid, thanks man` versus `card didn't work, lamer`, we can see that carders do have valid (and sometimes invalid) carding data. Thus, while we can't conclude why carders are willing to sell for $2 a card, we can conclude that sales are being conducted.

Further proof of such sales comes from banks who participate in underground markets and feed credit data into the market to see how quickly and where the card is later charged[7]. Rip-off reports, free valid credit data, and bank participation in monitoring underground networks offer tangible evidence to show underground markets do exist and the data being sold is real.

4.2 Market Reputation

In an economy based around anonymity where scammers can't be punished, reputation is all that separates a legitimate carder from rippers. In theory, verification hinges upon a participants continued access to fresh data and positive feedback from other market members. Yet there is nothing to stop a market owner from just granting verified access to a fellow scammer and cashing out on false sales while vehemently defending the ripper's reputation against charges of fraud. Similarly, dummy individuals can purport successful sales to raise a false credibility to a ripper's status. The alternative is equally possible; legitimate sellers can be slandered by other participants, forcing them to lose their status.

The potential for dishonest behavior gives rise to markets themselves having reputations. 'Good' markets are those where operators restrict access to verified status and try to maintain credibility, while 'bad' markets are prone to rippers and half-fulfilled sales. In order to defend integrity, some markets require new members to be vouched for by an existing member as an additional protection against scams (and possibly monitoring), in effect creating a web of trust. The existence of operators who verify sellers and chains of trust is reminiscent of certificate systems such as VeriSign and PGP. Whether good or bad, underground markets exist auctioning off stolen credit data; finding them is just a search away.

5 The Money Tree

Credit theft is not without risk. For underground participants living in countries with cybercrime laws, the threat of punishment by a federal authority is real [8]. To help reduce the possibility of illicit transactions trailing back to a participant's real identity, underground economies have adopted techniques of transferring funds and cashing out stolen accounts that are explicitly anonymous or unlikely to be logged. Discovery of new laundering techniques is an ongoing process as old methods fall out of favor or become inaccessible. Evasion of federal and banking authorities is thus a creative process pushed by underground participants looking to continually cash out on stolen credit identities.

In exploring the content of advertisements and tutorials available on a number of carding forums, we encountered a collection of techniques used by the underground economy to anonymously launder funds. While by no means a comprehensive list, each technique offers an insight into the thought process behind keeping transactions anonymous – successful or not.

5.1 Payment Methods

Obtaining services from the underground economy means payment, and by its rules. Advertisements we encountered often indicated the buyer or seller's preferred method of transferring funds including e-gold, Western Union, and to a limited extent, PayPal. Each of these services allow electronic transfers to other digital accounts or to individuals located anywhere on the globe. As account creation, login, and money transfers are handled exclusively online, there is no physical identity associated with laundered money other than an IP address. When used in conjunction with a trusted proxy, useful details about an account's owner can completely disappear.

While some companies have adopted more stringent requirements in the face of legal complications [9], inevitably the anonymity of the internet favors criminals. If a digital account is closed on suspicion of fraud, another can easily be opened with no apparent connection between the old and new account. So long as banks retain lax policies on account creation or insider threats exist, underground markets will have the tools necessary to launder money.

5.2 Cashing Out

With credit data in hand, underground participants need a means for dumping an accounts funds. The techniques for cashing out are continually evolving, but the following examples provide a survey of methods potentially exploited by underground miscreants.

Intermediate Shipping

The threat of linking a physical identity to credit fraud by shipping illegally purchased goods to a home address has given rise to market participants (drops) providing intermediary shipping addresses across the globe. Drop operators offer to accept goods under guise of a stolen card's owner, after which they re-ship the goods to the purchaser's final destination of choice. Other participants, unwilling to deal with the associated fee of hiring a drop, elect to set up their own personal drops by enlisting the help of unsuspecting individuals.

In the case of a participant starting his own drop, underground forums provided a list of suggested techniques used by drop operators including (1) renting another individual's mailbox, (2) setting up a front company that offers 'remote employment' where by employees then forward illegally purchased goods, (3) scamming individuals on social networking sites such as MySpace to forward packages they receive, and (4) shipping goods to a friend's address. The risk associated with any of these endeavors is outside the scope of this paper, but the techniques elected show the creativity (or ignorance) of participants in circumventing the threat of federal authorities.

Western Union

Western Union, detailed earlier as a method for paying sellers for stolen data, can also be used for cashing out accounts provided enough details are known about the stolen credit card owner's identity. Western Union requires that money orders with a credit card originate in the card's country of origin if the order is produced by phone. This leads to market participants advertising their willingness to pose as the card owner, often requiring a male or female voice. While digital transfers circumvent this necessity, both physical and digital money orders dealing with sums in excess of $1000 require one of the following: a passport number, social security number, or drivers license number. Such requirements imposes a higher cost of entry as normal CVV2 data sets are limited to a billing address and authentication code. Thus, while Western Union poses a possible means to launder funds, the cost of entry is higher than other alternatives.

Online Gambling

Rather than risk dealing with untrusted entities, market participants have adopted using web services to obscure the origin of laundered money. Of the methods detailed by underground participants, online gambling presents a low-cost means of transferring money from one account to another with little risk of activities being logged and tracked down. In the presented scenario, two players would sign up for new accounts with an online gambling group, one member (`l0ser`) attaching stolen credit credentials while the other member (`w1nn3r`) uses a card attached to the account funds are destined to be laundered. The `l0ser` and `w1nn3r` proceed to enter a private game where the `l0ser` throws every game until the stolen credit card is maxed out. The `w1nn3r` then claims his earnings from the gambling site which are transfered into the legitimate account. The gambling host thus acts as a layer of obscurity between the stolen credit card and the participant's account.

Intermediate Banking

While never explained publicly in any of the underground economies monitored, certain market participants purported their ability to transfer funds from

bank account to bank account provided enough information. Such activities require some semblance of authenticity with the banks funds are being transfered between. Whether such participants are honestly reporting their abilities or not is beyond the capability of this report to address, but insider threats pose a major hurdle in defeating credit and identity fraud.

5.3 The Cost of Fraud

Identity theft is a sophisticated form of white-collar crime, and as such it's often difficult to tell who bears the real economic losses when it occurs. One important factor is the type of data (bank login, credit card, full personal details) that the criminal used to complete a fraudulent transaction.

When a consumer uses a credit card to pay for something, a complex transaction is initiated between at least four parties: the consumer, the card's issuing financial institution (Chase, Bank of America, etc.), the merchant, and the payment network (Visa, Mastercard, etc.). Regardless of whether the card is present at the point of sale (most brick-and-mortar merchants) or not present (most Internet transactions fall into this category), the transaction begins with the merchant using the payment network to requesting payment from the consumer's issuing bank. The issuing bank has the choice of either approving or denying a transaction; if an approval is issued, the bank has agreed to remit payment on behalf of the consumer to the merchant.

However, credit card sales can be disputed. In the case of a dispute, the burden of proof generally lies with the merchant, who must prove that the details of the transaction took place as they reported them to the bank: that the person using the card was the cardholder, that the merchant performed their obligations to the cardholder, etc. Barring any of these conditions, the bank reserves the right to refuse payment to the merchant, in which case the merchant will not receive payment, although they have likely already shipped goods and/or delivered services to the person who purported to be the cardholder.

> B̈anks that issue the credit cards don't cover the cost of the scams. "We don't take any loss via the Internet because we can charge it all back [to the merchant] using Visa and MasterCard rules. The merchant, not us, bears the cost," said Rob Milson, manager of fraud operations at Mellon Bank in Pittsburgh." [1]

With other forms of data, it's less clear who bears the cost of fraud. We suspect that individuals would be more responsible if their full identities are stolen (date of birth, Social Security number, etc.) but did not investigate this area thoroughly. Likewise, it's not clear who bears the loss if bank login data is used fraudulently.

6 Sophistication: l33t or n00bs?

Carders, cashiers, drops, bank insiders, credit fraud, and evading federal authorities; the details of the underground economy thus far offer the impression of a highly systematized and thriving economy of credit card theft. Yet the question remains, how sophisticated are the individuals participating in underground economies?

Gullibility and treachery were addressed in Section 4, yet an important question for researchers designing security protections is the technical competence of underground participants. An equally important question for law enforcement is how savvy miscreants are at circumventing fraud monitoring. Where strict measurements can be applied to monitoring market activity and the services being sold, understanding criminal sophistication falls on the highly subjective. We thus motivate the issue with a number of examples that highlight the spectrum of sophistication found in market participants.

Hopelessly Unaware

At the far left end of the spectrum are the hopelessly unaware, the individuals gullible enough to purchase credit data from random sources with no credibility (if such a term can ever be applied) or members who are just entering the credit fraud circle. Such individuals are plagued by questions of what a cvv2 is, what a proxy is, or could someone please send a free cvv2 plz? Sometimes more pointed questions appear asking whether using stolen credit data is illegal or not. Regardless the questions, market forums and channels are full of individuals who have yet to master the ins and outs of credit fraud.

Risk Unaware

A step ahead the hopelessly unaware are those buyers and sellers who know how to play the game of credit fraud, but are prone to taking risks without necessarily recognizing the danger. While tutorials are readily available for how to get started on carding ones first Xbox 360, in monitoring underground marketplaces we saw threads and conversations dealing with individuals who would use their friends house as the shipment address for illegally purchased goods or buyers who would

use stolen credit cards to order pizza – to their own home. Other members of this category, perhaps not quite as unaware as others, include those participants who fail to use proxies when dealing with illicit transactions or who use their own phone for making deals.

Risk Averse

The final right end of the spectrum includes the risk averse, market participants who always access carding sites and channels through proxies, use skype to obscure phone records, and use trusted drops or cash out methods to prevent any readily available links from forming between the participants' real identities and the illicit transactions they conduct.

While these classifications provide insight into the breadth of market participants, the conversations where miscreants spoke of their protection measures were few and far between. Our own data lacks enough volume to make a conclusive statement, but by measuring the number of messages dealing with buying and selling vs. requests for help and tutorials vs. scam reports on a single forum, we found that help requests comprise a large part of network traffic. These results cannot necessarily be generalized across all markets, however, it is within reason to claim this particular market generates a large amount of traffic from unsophisticated participants.

Forum Post Volume	
Buy/Sell Advertisements	3140
Tutorial Questions	1207
Scam Complaints	840

7 Defeating the Underground?

Sophistication plays heavily in the prospect of defeating underground markets. If credit data is stolen by highly efficient phishing scams and zero-day flaws, the plausibility of defeating the underground seems slim. Alternatively, if participants target outdated flaws that will eventually be patched, it is possible markets will dry out. The realistic situation for underground markets lies somewhere between these two extremes, yet regardless the sophistication, all markets rely on five resources: fresh credit data, network access, trust, laundering sources, and to an extent internet-user naivete. We examine the viability of targeting access to each of these resources and the resulting market effects.

7.1 Targeting Credit Sources

Continued access to fresh credit data is the foundation of underground economies. Without credit cards to sell, markets will have nothing to sell and subsequent service providers will be hard press to find customers. Disabling access to credit data requires knowing where it originates. During our monitoring, the majority of credit cards posted to channels included a processing or sale id number, alluding that the card was stolen from a shopping cart database. Regardless of how the database is being stolen, credit companies require merchants to follow PCI DSS standards, including not storing CVV2 numbers [10] [11].

Without the CVV2 data, buyers are unable to use stolen cards unless they guess the 3-4 digit number, a 1/1000 or 1/10,000 chance. Requiring merchants to follow standards thus stands as a low-cost protection in defeating underground markets, forcing miscreants to target live transactions defended by encryption or to play a guessing game. However, securing databases is not the panacea of credit fraud. Phishing and cross-site scripting pose additional threats to stealing credit data as well as employees handling card data. Nonetheless, properly storing data and securing databases is a strong first step in defeating fraud.

7.2 Targeting Networks

The numerous participants that meet in networks to hawk services raises the possibility of shutting down access to market meeting grounds. Despite seeming a logical solution, however, shutting down networks requires a great deal of legal wrangling. Domain names, hosting, and restrictions there of differ across the world. While terminating a market running out of the United States may be easy, markets in other countries without cybercrime laws are beyond law enforcement to touch. The alternative of circumventing laws and agencies and using methods such as denial of service instead is illegal. Whether or not fraud is covered under free speech is beyond this report, but the legal challenges of restricting access to forums and IRC channels remains outside of reason in the current legal blackhole of the internet. Thus, while markets remain an integral resource to credit fraud, they are beyond targeting at this point in time.

7.3 Targeting Credibility

Trust, as detailed in Section 4, plays an important role in a buyer's willingness to do business with a seller. In their own analysis of underground markets, [3] suggested the possibility of launching a sybil attack on

verified users. The success of such an attack is highly dependent upon the requirements of achieving verified status. If the hope is to masquerade a verified user and later perpetrate scams, each sybil identity must fist pay a fee and then provide access to a number of valid credit cards. Harvesting these cards from rival markets is likely implausible due to the speed at which they are cashed out and invalidated, thus each identity must also have access to fresh data. Lastly, a reputation needs to be built by selling actual data within the markets which is subsequently reported by other members. Without bank participation, selling credit data will either be illegal or highly costly to the sybil attacker.

Similarly, attacking the credibility of current verified members requires other market participants to trust each sybil identity. Most ripper reports require screen shots of conversations and a proof of transaction. If fake copies are produced, other market participants will chime in their own opinion whether the verified user is a scammer or not.

The potential of sybil attacks is largely reduced in a reputation system that acts as a web of trust. Creating new identities and entering the market will be slowed by requirements of only vouching for one other participant and new participants being forced to wait a number of weeks before vouching for another member. Thus, while a sybil attack may be valid against smaller networks where trust is an issue, larger market places that have systematized trust systems will be far less susceptible. In either case, however, there are certainly legal questions that would need to be addressed pertaining to dealing in stolen credit data.

7.4 Targeting Laundering

For payment to occur or credit cards to be cashed out sources of laundering funds must exist. The difficulty of defeating laundering falls into the same legal realm as shutting down networks; different countries have different laws. A participant using stolen credit cards to purchase goods in Nigeria which has no extradition laws is beyond the reach of federal authorities in other countries. Thus, while laundering resources are an important target in defeating fraud, the plausibility of enacting barriers and the associated legal challenges is beyond this report.

7.5 Targeting Naivete

Naivete in the internet poses a major hurdle in defeating credit fraud. The fears and skepticism present in physical transactions and sales are entirely different than those encountered in digital business. Why does an email from a bank illicit a response with credit data while a man dressed in a suit with a brief case purporting his association with a bank goes entirely untrusted? Whether or not the golden-lock icon will save the internet remains to be seen, but until that point, phishing and similar scams that prey upon the gullibility of the current internet generation will continue to succeed.

8 Conclusion

A thriving marketplace exists to facilitate the transfer of goods and services in the underground economy. Buyers, carders, cashiers, drops, and rippers participate in IRC channels and bulletin boards which act as the underground economy's rendez-vous and bargaining locations. Many goods traded in these markets relate to identity theft directly (fulls, credit card data, bank logins), but they also serve as a forum for trading diverse goods including compromised machines and spam services. The markets employ measures to ensure honest participation, but some treachery does exist, both by users of the market, and sometimes the marketplace itself. The users of these markets range in sophistication from very inexperienced to seasoned, risk-averse criminals who work to maximize their returns while reducing their risk of getting caught.

How best to combat identity theft is an open question. Ethical and legal concerns dampen many routes that could potentially inhibit the underground economy. Alternatively, marketplace can serve as a useful tool for law enforcement agents to monitor fraudulent activity. In the end, the best methods in protecting credit data is to secure its storage and educate the current internet generation of the threats of identity theft. So long as there is money to be made by scams and exploits, the underground economy will continue to exist. One click, and countless identities can be owned.

References

[1] Federal Trade Commission. About Identity Theft. `http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html`.

[2] Joseph Pereira. How Credit-Card Data Went Out Wireless Door. `http://online.wsj.com/article/SB117824446226991797.html`.

[3] An Inquiry Into the Nature and Causes of the Wealth of Internet Miscreants. ACM, 2007.

[4] Honeynet Project. Know Your Enemy - A Profile. http://www.honeynet.org/papers/profiles/cc-fraud.pdf.

[5] Meet The Hackers. 2006. http://www.businessweek.com/magazine/content/06_22/b3986093.htm.

[6] Cybercrime Flourishes in Online Hacker Forums. 2006. http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm.

[7] To Catch an ID Thief. 2007. www.msnbc.msn.com/id/17805134/.

[8] FBI Tightens Net Around Identity Theft Operations. http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110201579.html.

[9] Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting. 2007. http://www.usdoj.gov/opa/pr/2007/April/07_crm_301.html.

[10] PCI Security Standards Council, LLC License Agreement. https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm/.

[11] Rules for Visa Merchants. http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf.