Characterizing Credit Card Black Markets on the Web

Vlad Bulakh*
vbulakh@cs.indiana.edu

*Indiana University
Bloomington, IN
United States

Minaxi Gupta*†
minaxi@cs.indiana.edu

†Edmodo Inc.
San Mateo, CA
United States

ABSTRACT

We study carding shops that sell stolen credit and debit card information online. By bypassing the anti-scrapping mechanisms they use, we find that the prices of cards depend heavily on factors such as the issuing bank, country of origin, and whether the card can be used in brick-and-mortar stores or not. Almost 70% of cards sold by these outfits are priced at or below the cost banks incur in re-issuing them. Ironically, this makes buying their own cards more economical for the banks than re-issuing. We also find that the monthly revenues for the carding shops we study are high enough to justify the risk fraudsters take. Further, inventory at carding outfits seems to follow data breaches and the impact of delayed deployment of the smart chip technology is evident in the disproportionate share the U.S. commands in the underground card fraud economy.

Categories and Subject Descriptors: H.3.5 [**Online Information Services**]: Web-based services; J.4 [**Computer Applications**]: Social and behavioral sciences

General Terms: Credit card fraud; data breach; black markets; underground economy; online fraud

Keywords: Stolen credit cards; dump; CVV; smart chip; EMV

1 INTRODUCTION

A large number of data breaches, including, Anthem [1], Target [2], Sony [3], Home Depot [3], Staples [3], Kmart [3], and Michaels Stores [3] have occurred in the past year. As a result, millions of consumers' financial and medical information has been exposed to cyber criminals, who can use the information for financial, political, and other types of gains. The most common impact of these breaches is the theft of credit card information, which can then be traded in underground black markets on the Web [4, 5].

Underground black markets are efficient. The first batches of stolen credit card information from the Target and Home Depot breaches became available for sale almost immediately after the breach was first reported. The illegal markets are also nimble. As law enforcement shuts down the servers hosting online marketplaces and arrest the criminals responsible for the security breaches, thieves find new ways to thrive, often by switching hosting providers in the blink of an eye. During our study, an online marketplace, `rescator.so`, changed domain names twice: it shifted from `rescator.so` to `rescator.cc` sometime around July-September 2014, and it later changed to `rescator.cm` at the end of November 2014.

WWW 2015 Companion, May 18–22, 2015, Florence, Italy.
ACM 978-1-4503-3473-0/15/05.
http://dx.doi.org/10.1145/2740908.2742128.

There already have been a few studies related to the credit card fraud economy. Previous research [6, 7] studied underground marketplaces for credit card fraud, identity theft, spamming, phishing, online credential theft, and the sale of compromised hosts. Much has changed since these studies, including the usage of IRC (Internet Relay Chat), which significantly declined over the past decade. Since these studies were broader in scope, they did not focus on credit cards in particular. More recent work [8] has focused on online credit card black markets. We complement their preliminary work by studying debit cards in addition to credit cards, and also by dissecting the evolution of these marketplaces and the evasion tactics they employ longitudinally.

In this paper, we undertake a measurement study of three online carding shops – `rescator.cm`, `dumps.pw`, and `2pac.cc` – that sell stolen credit and debit cards. Our approach was to register at these marketplaces and collect publicly available information to understand their inventory and revenue, among other things. This gave us many insights into the operations of a typical Web-based carding shop. Note that we chose not to purchase any of the credit cards offered for sale due to legal reasons [9, 10], even though it would have been interesting to understand the credit card fraud economy end to end. Our work can not only guide defense strategies for issuing banks and merchants but also serve as a benchmark for the effectiveness of smart chip technology (often referred to as EMV) [11], which makes it practically impossible to clone stolen credit cards as the deadline for its adoption approaches. The key findings from our work are the following:

- Factors impacting prices: We discuss the impact of the issuing bank, the card type, the country of origin, and other factors on the prices of credit and debit cards sold on the black market. For example, we find that credit cards are not only more popular than debit cards in online carding shops, but they also cost 22% more.
- It is cheaper for banks to buy: Issuing new cards following a breach costs money and creates an inconvenience for the consumer. Somewhat surprisingly, we observe that almost 70% cards sold are priced at or below $10.00, which is the cost issuing banks incur. Though not recommended, ironically, this makes buying their own cards more economical than re-issuing.
- Online carding shops are thriving: The monthly revenues for carding shops we studied ranged from $181K-277K per month, suggesting that criminals find the pursuit lucrative enough to justify the risk.
- Smart chip helps: Cards issued in the U.S. command a disproportionately higher share at all carding shops, implying that countries where smart chip technology has been deployed are reaping the anti-cloning benefits offered by the technology.
- Anti-scrapping mechanisms are heavily used: One of the carding shops we study requires one to solve a CAPTCHA approximately every 100 minutes of continuous browsing. Two more shops monitor if requests are originating from a browser. These impediments posed numerous technical difficulties in data collection, and we had to constantly adapt the scraper to keep up.

- Inventory follows breaches: We find evidence that the inventory of stolen cards at the carding shops increases immediately following breaches, pointing to the efficiency of such outfits.

2 BACKGROUND

We will use the generic term "card" to refer to both credit and debit cards throughout this paper. Here, we provide an overview of the fraud pipeline and position the scope of our study.

2.1 Fraud pipeline

The fraud economy surrounding credit and debit cards can be thought of as a four-step pipeline. The first step in this pipeline is the *theft* of either card information or the physical card. The latter is less common. Cyber criminals achieve the former in various ways. The common techniques used in the security breaches of the last year included placing malware at the point-of-sale (POS) system used to swipe cards at brick-and-mortar stores, and infiltrating servers storing customer information. Card skimmers – devices used to steal card information during physical transactions at gas pumps, automatic teller machines, etc. – are also common.

Carding shops then acquire the stolen cards or information and offer them for sale [4]. The *acquisition* of the stolen data is the second step of the pipeline. The focus of this paper is the third step of the pipeline, where carding shops place stolen card information up for *sale*. Carding shops offer two types of debit and credit cards. First, a **dump**, is card information stolen from physical locations, such as POS devices. Their output contains enough information to clone a card's magnetic track, writers for which can be purchased easily for under $400 (for example, Unitech MSR206 [12]). Dumps can only be used to produce physical cards that must be used at brick-and-mortar stores [13, 14] because they lack information generally known only to the cardholder (e.g. billing address). The second type of cards sold at carding shops are referred to as the **CVV**. Such cards contain credit/debit card information stolen from an online merchant. CVVs can only be used for online transactions since they lack magnetic track information needed for producing physical cards [14].

In the final step, people who purchase a credit or debit card from a carding shop try to *monetize* it by making unauthorized purchases.

2.2 Carding shops

At first glance, a carding marketplace resembles a legitimate shopping website. There is a main page showing the latest card availability, price drops, and website news. There is also an account page where the user can change their username/password combination and view past purchases. Search engine integration on product pages allows visitors to find what they are interested in. The only difference from a typical legitimate online shopping website is that the products offered for sale by these shops are not legitimate. Perhaps as a consequence, most carding shops only accept payments via virtual currencies, such as Bitcoin and Litecoin, which allow for secure transactions that are not only impossible to reverse, but also do not contain any personal information. Although some carding shops accept alternative forms of payment from outlets such as Western Union, they usually require a large minimum deposit ($400 or more) and accept cash only. Furthermore, as an added security measure, most currency transfers that are not done via virtual currencies are required to be sent to a third party, a *dropper*, who then delivers the money to the merchant, which makes it more difficult for the authorities to trace the money and incriminate fraudsters. The involvement of a third party is the most likely reason behind the large minimum deposit requirement since it would make little sense for the dropper to pick up small bills.

Carding shops do differ from legitimate websites in other ways. First, they all seem to feature mandatory account registration. Most even require visitors to solve a CAPTCHA before allowing them to view cards for sale. Furthermore, many outfits have begun using CloudFlare's content delivery network and DDoS protection services [15], which makes their websites more difficult to scrape since all HTTP GET requests that are not being issued from a browser are blocked by CloudFlare.

Finally, many carding shops do not allow their visitors to view any product pages without a minimum deposit. The deposit requirement limited our options for scraping significantly. Still, we found three popular carding shops that did not require a deposit for this study and collected a respectable amount of data.

2.3 Smart chip

A sea technical change in the credit card industry is in the works in the U.S. Smart chip-enabled cards feature embedded electronic chips that uniquely encode each transaction, making it more difficult for miscreants to counterfeit or copy such cards. According to a number of reports, countries that adopted smart chip technology saw a significant decline in credit card fraud [16, 17]. Still, as some studies point out [18, 19], smart chip technology is far from being flawless, and miscreants can exploit its weaknesses. It is expected that as many as 70% of credit and 41% of debit cards in the U.S. will have smart chips embedded in them by the end of 2015 [20]. Security researchers and practitioners would surely be interested in seeing the fraud situation evolve post smart chip card deployment in the U.S., for which our paper can serve as a benchmark.

3 DATA COLLECTION AND ANALYSIS METHODOLOGY

3.1 Data collection and challenges

Although there are a number of differences across various online carding shops, they all feature the same basic structure – a news page describing data availability from the latest breaches and other website news, an account page where a person can see past purchases and deposit money to their account, card dump pages that list all credit and debit card dumps that are available for sale, CVV pages which lists all online-only cards that are available for sale, and a card check page which allows the customer to test the validity of the purchased credit and debit cards. We limited our data collection efforts to three types of pages – the news page, card dump pages, and CVV pages – since this is the minimum set that provides useful insights without treading into illegal territory.

Our initial data collection effort dates back to July 30, 2014, when we began scraping two carding shops: `2pac.cc` and `rescator.cm`. Those two websites were chosen primarily due to their relatively high Alexa rankings and similar web page structure. We wrote a scraper in Python that would scrape those websites 24/7 by issuing HTTP GET requests for each page containing the data. Since both carding shops required the solution to a CAPTCHA before entering the websites, we had to manually solve a CAPTCHA at the beginning of each scrapping session, after which the scraper would take over and authenticate with our username and password, and then use the same browsing session to access the data.

To our surprise, both websites regularly went offline during that time period for unexplained reasons. Still, everything went relatively well until both shops started using CloudFlare as their content delivery network at approximately the same time. CloudFlare detected our scraper and would not let us collect any data. We changed the user agent used by the scraper, tried to send all HTTP GET requests via Python's *urllib* instead of the *Requests* library in case there was a bug in the latter, and even tried converting the scraper to Java to see if it would make a difference, but to no avail. Since both carding shops were still working from a web browser,

we decided to change our strategy and use the *Selenium* library which allows one to automate web browsing and scraping.

The new strategy worked – CloudFlare was unable to detect our scraper when it ran a Firefox browser in the background and collected all information from there. Unfortunately, shortly thereafter 2pac.cc went offline due to the arrest of its owner [21, 22]. It was still offline at the time of this writing.

After waiting for 2pac.cc to come online for some time, we started to look for replacements. Unfortunately, most of the carding shops were either abandoned, were offline, or required an initial deposit in order to view the contents. We eventually chose dumps.pw as it seemed to be the best of the options. Similar to 2pac.cc and rescator.cm, dumps.pw requires visitors to solve a CAPTCHA before allowing them to access the website. In what seems to be an effort to prevent people from scraping their website, dumps.pw also requires the users to solve a CAPTCHA and re-enter their credentials approximately every 100 minutes of continuous browsing, which significantly complicated scraping since someone had to be constantly solving the CAPTCHAs every 100 minutes (we could have collected the data for just under 100 minutes at a time, took a break, and then resumed, but that would have resulted in the scraper missing the cards that would have been added and sold during the break). We still managed to collect data from dumps.pw, albeit not as much as from rescator.cm.

In the end, we collected data for two time periods: 07.30.2014-08.27.2014 for rescator.cm and 2pac.cc and 10.28.2014-present for rescator.cm and dumps.pw. Due to a hard disk failure, we lost some of the data collected from 2pac.cc. Also, the dumps.pw data collection began on 11.19.2014. Table 1 summarizes the data we collected.

Carding shop	Days	Unique cards	Average price	Daily revenue
rescator.cm (time period 1)	29	19,844	$8.78	–
2pac.cc	1	1,525	$20.64	–
rescator.cm (time period 2)	96	58,684	$9.73	$6,034.90
dumps.pw	79	73,383	$11.66	$9,226.10

Table 1: Summary of data collection

3.2 Data description

All carding websites we crawled allow visitors to see limited amount of information about the credit and debit cards in their databases before making a purchase. The quality and quantity of displayed information varied significantly across the three outfits.

CVVs: Most carding shops show the following information about each CVV to their visitors: BIN (Bank Identification Number), card brand (Visa, Discover, Amex, etc.), card type (credit versus debit), card mark (Platinum, Classic, Prepaid, etc.), expiration date, country, state, city, zip, base name[1], price. Naturally, not all this information is needed to complete an online transaction. The reason for providing base names as well as brands and marks of cards is to allow customers to make an informed purchase. For example, it is easier for someone to 'cash out' a CVV if they live in the same city as the original owner of the card since an online order would raise less suspicion if there is only a minor difference (i.e. street name) in billing and shipping addresses.

Dumps: The vast majority of carding shops show the following information about each credit and debit card dump to their visitors: BIN, card brand, card type, card mark, expiration date, Tracks 1 or 2 present[2], country, issuing bank. Similar to CVVs, information such as issuing bank and country of origin is not required to make a purchase in brick-and-mortar stores, and the only reason that it is provided is to give potential customers the availability to pick and choose cards that will bring them the most revenue.

As for differences in information shown across carding shops, although dumps.pw shows the last four credit/debit card digits to their customers before the purchase, neither rescator.cm nor 2pac.cc provided that information. In addition, all three websites seem to be assigning unrelated base names to the cards that they are selling. For example, "SILVER_WORLD2" and "SILVER_JULY14_HUGE" for 2pac.cc, "2 october arkansas" and "14 october new york" for dumps.pw, "American Sanctions 13" and "European Sanctions 2" for rescator.cm. Such differences make it difficult, and in some cases impossible, for one to analyze the data and make valid comparisons since there is no way to recover the omitted debit card brand on rescator.cm or infer the last four digits of a credit card sold by 2pac.cc without making a purchase. In order to account for these issues without discarding any data, we manually labeled all impossible to resolve cases as 'other', which is also how we labeled all infrequently occurring card brands, issuing banks, and countries of origin.

3.3 Data sanitization

We use the term *snapshot* to refer to an iteration of our scraper subsequently in this paper. Under ideal conditions, it would give us an exact copy of all data available at a carding shop at that point of time. Overall, we collected 4,063 snapshots for rescator.cm and dumps.pw. We were also able to collect three snapshots from 2pac.cc. Out of these, two-thirds of the snapshots were usable. The rest were discarded due to the incompleteness resulting from the following problems: 1) Hosting problems for rescator.cm and dumps.pw, which required us to manually restart the scraper; 2) Updates at carding shops, which resulted in incomplete snapshots; and 3) Internet connection problems on our side.

We also saw a number of inconsistencies in the collected data, even when the data is from the same carding shop. For example, the bank field could say "JPMORGAN CHASE BANK", "CHASE BANK USA", "JP MORGAN CHASE BANK", or "CHASE BANK", all of which are obviously the same. Information could be omitted. For example, any combination of city, state, zip, country could be missing. We also saw a number of incorrect entries. For example, text in the *country* field could read "United Kingdom, CA, Los Angeles, 90065", which cannot possibly be correct since Los Angeles, CA 90065 is located in the U.S. and not in the United Kingdom. Another example is an entry for a credit card where "68" is the *last four digits* and 13/17 is an *expiration date*, both of which are obviously incorrect because 68 is two digits and there are only 12 months in a year. All the above suggest that the card information entry has a manual component. In addition, the inconsistencies were themselves inconsistent which implies that there are multiple people inputting the data.

Due to the low quality of the data, much time and effort was spent on data sanitization. About 15% of the data we collected had to be cleaned up, which, amongst other things, involved standardizing the names of the countries, banks, etc. (e.g. both "Amex" and "AMERICAN EXPRESS" became "American Express"), inferring missing information (i.e. determining the country if only the city and postal/zip code are known), and ignoring invalid entries.

4 DATA ANALYSIS

After cleaning up the data collected from 2pac.cc in July-August 2014 and rescator.cm and dumps.pw in October 2014-February 2015, we totaled 133,592 unique credit and debit cards, all of which are used in this section. We also have a July-

[1]Card base name is a name/label/code word assigned to a particular batch of stolen credit or debit cards by the miscreants.

[2]Tracks 1 and 2 are magnetic tracks on credit and debit cards that contain information used for financial transactions

August 2014 rescator.cm data set containing 19,844 unique cards, which we only use for temporal comparison (Section 4.7).

4.1 Volume of cards and estimated revenue

Between October 2014 and February 2015, rescator.cm sold 56,976 credit and debit cards (7,784 of which are dumps and 49,192 are CVVs) while dumps.pw sold 55,784 card dumps during a slightly shorter time frame. According to our estimates, the average price of a dump sold on rescator.cm is $16.25 while the average price of a CVV is $8.47. In addition, we calculated the average price of a credit/debit card dump sold on dumps.pw to be $11.66. Using this knowledge we estimate the gross revenues of rescator.cm and dumps.pw to be $6,034.90 and $9,226.10 per day, respectively. This translates to $181,047 and $276,783 per month for rescator.cm and dumps.pw, which seems to justify the risk cyber criminals are willing to take by engaging in this illegal activity. Also, although it would have been nice to know the revenue of 2pac.cc, we were unable to make an estimate since their website is currently offline, and we only have one day of usable data to work with.

To compute revenues, we used the observation that rescator.cm and 2pac.cc assign a unique ID to each card in their shops, but dumps.pw does no such thing. We used all available data fields as an artificial ID for all cards sold by dumps.pw, which resulted in undercounting since there was more than one card with the same last four digits, country, issuing bank, and expiration date. As a result, the actual revenue of dumps.pw is probably much higher than our conservative estimate.

4.2 Credit vs. debit cards

According to our data (Table 2), the average price of a card sold on rescator.cm, 2pac.cc, and dumps.pw is $10.92, with credit cards generally being more expensive than debit cards ($12.17 vs. $9.52). This finding is a little surprising, especially considering that: 1) Most credit cards have somewhat low credit limits; 2) a person's bank account could, in theory, contain a person's life's savings, all of which could almost instantaneously be withdrawn using that person's debit card information; and 3) most credit cards offer more protection to consumers than debit cards.

Type	Total # of cards	Avg. price per card (total)	Avg. price per card (rescator.cm)	Avg. price per card (dumps.pw)	Avg. price per card (2pac.cc)
Credit	66,069	$12.17	$9.66	$15.33	$30.02
Debit	53,722	$9.52	$10.00	$9.16	$16.50
Unknown	13,782	$10.36	$9.20	$10.67	$15.45
Other	19	$11.58	$12.00	$10.00	n/a

Table 2: Card prices by type

It reportedly costs banks approximately $10.00 to reissue a credit card [23]. In addition, a 2014 report [24] by the American Bankers Association says that, on average, banks lose $331 per stolen debit card and $530 per stolen credit card. If we combine this knowledge with the fact that 69.95% of credit and debit cards sold by rescator.cm, 2pac.cc, and dumps.pw are priced at or below $10.00, the banks might actually be better off just purchasing some of their cards from the carding shops, assuming, of course, that the shops can be trusted to completely remove the card information from their databases once a card has been sold.

Another surprising finding was that there are almost twice as many credit cards as there are debit cards in the rescator.cm shop while the opposite is true for 2pac.cc and dumps.pw. In addition, approximately 10% of the cards sold by all three shops were not identified as either credit or debit. The average price of such a card is $10.36, which makes unidentified cards more expensive than debit cards but cheaper than credit cards. Obviously, an unidentified card could turn out to be either a credit or a debit card; hence, it makes sense for such cards to be priced the way they are since, at the very least, the buyer would be purchasing a debit card (which costs less), but could possibly get a credit card (which is more expensive).

4.3 Card brands

Here, we look at how the brand of a card affects its price. As can be seen from Table 3, MasterCard (MC) credit and debit cards are more expensive than the rest, with the average price being $13.64 per card. Discover cards take a distant second place, closely followed by Visa and Maestro. On the other side of the spectrum we have American Express (Amex) cards, which tend to have the lowest price of all major credit/debit card brands. The premium price of MasterCard-branded credit and debit cards could be due to the fact that MasterCard is the most widely accepted card in the world and boasts more automatic teller machines than any other network [25].

We also observe that carding shops tend to have more than three times the number of Visa cards in their possession than any other brand. One of the explanations for this phenomenon is that more people have Visa credit and debit cards than those of any other brand [26]. In addition, Visa is not known for its outstanding customer service [25], which could indicate it might be more difficult and time consuming for the customer to notify the fraud department about a stolen credit card, all of which plays into the hands of the miscreants. Finally, we observe that rescator.cm and 2pac.cc usually offer at least twice as many MasterCard-branded cards as American Express cards while the number of cards of both brands is almost always the same on dumps.pw.

Brand	Total # of cards	Avg. price per card (total)	Avg. price per card (rescator.cm)	Avg. price per card (dumps.pw)	Avg. price per card (2pac.cc)
Visa	79,804	$10.30	$9.41	$10.99	n/a
MC	25,978	$13.64	$11.32	$15.79	$24.89
Amex	18,503	$10.16	$8.17	$11.52	$15.89
Unknown	6,730	$9.95	$11.59	$9.76	$14.51
Discover	2,169	$10.41	$10.02	$12.39	$18.68
Maestro	372	$10.35	$10.58	$6.84	$14.53
Other	36	$9.92	$10.91	$9.26	$12.00

Table 3: Card prices by brand

4.4 Card mark

A card type (also called *mark* and *level* in underground marketplaces), such as Classic, Standard, Platinum, and Signature, determines maximum credit limit, annual percentage rate (APR), and annual fee, as well as various perks and benefits the cardholder is entitled to receive. In addition, although it is relatively simple to acquire a no-thrills, basic Visa card with a high APR, low credit limit, and no perks, most banks will require the applicant to have a high credit score along with a hefty yearly income in order to qualify for one of their premium cards with high a credit limit, generous reward program, and better customer service.

Mark	Total # of cards	Avg. price per card (total)	Avg. price per card (rescator.cm)	Avg. price per card (dumps.pw)	Avg. price per card (2pac.cc)
Classic	31,344	$7.73	$7.95	$7.61	n/a
Unknown	26,912	$9.69	$8.68	$10.06	$14.80
Platinum	26,376	$12.64	$11.03	$13.93	$22.00
Signature	10,763	$11.54	$8.21	$22.55	n/a
Standard	7,094	$9.80	$10.25	$8.72	$14.31
Premier	6,057	$12.88	$12.36	$13.57	n/a
Business	5,871	$18.14	$12.90	$21.84	$34.32
Prepaid	4,453	$7.59	$8.42	$7.43	$14.44
WorldCard	3,312	$14.34	$9.86	$24.38	$39.00
Gold	3,092	$14.42	$12.84	$16.41	$21.25
Other	8,318	$14.19	$10.21	$16.70	$32.20

Table 4: Card prices by mark

When looking at the marks of credit and debit cards, we see that Classic, Prepaid, and Standard cards are the cheapest of the group,

with Prepaid cards being the least expensive with an average price of $7.59 per card (Table 4). On the other side of the spectrum we see Business, Gold, and World Card, all of which are the first, second, and third most expensive cards, respectively. The cheapest cards in the list are very common in the U.S. and can be acquired by virtually anybody with a decent credit history. More expensive cards, on the other hand, are not as common, more difficult to attain, and are usually owned by people with higher average incomes, all of which results in higher credit limits and more opportunity for a large purchase going unnoticed by the bank's fraud department. Naturally, this warrants a premium price tag. Interestingly enough, `dumps.pw` usually has more Standard than Signature cards for sale while the situation is reversed for `rescator.cm`, which almost always has three times as many Signature cards in stock.

4.5 Country of origin

We find that 82% of all credit and debit cards sold by `rescator.cm`, `dumps.pw`, and `2pac.cc` have been issued in the U.S. (Table 5), which is hardly surprising considering that not only have almost all recent data breaches happened in the U.S., but, unlike its European counterparts, the U.S. has yet to transition to the smart chip EMV technology, which offers significantly better anti-cloning protection than the magnetic strip-based cards. What is surprising, however, is that a typical U.S. credit/debit card costs less (as much as 200% less in some cases) than some cards issued in countries such as Canada, Australia, Germany, and Thailand. One possible explanation for this could be that banks in the U.S. feature better fraud-detection mechanisms, which means that there is less chance that an unauthorized transaction will go through. Interestingly enough, the most expensive cards are from Nepal ($80.00 per card), Paraguay ($70.00 per card), and Nicaragua ($54.72 per card), while the least expensive cards come from India ($6.22 per card) and Israel ($6.83 per card). One reason for such low prices could be that credit cards issued in India and Israel have lower credit limits compared to credit cards issued in the U.S. and other countries.

Country	Total # of cards	Avg. price per card (total)	Avg. price per card (rescator.cm)	Avg. price per card (dumps.pw)	Avg. price per card (2pac.cc)
U.S.	109,760	$10.25	$8.97	$11.17	$20.90
Unknown	6,734	$10.07	$13.58	$9.87	$14.51
UK	4,226	$9.11	$13.32	$8.70	$32.50
Canada	2,888	$12.39	$16.54	$10.72	$64.82
Australia	880	$23.76	$12.80	$46.15	n/a
Other	9,104	$18.69	$14.92	$26.10	$30.00

Table 5: Card prices by country of origin

4.6 Issuing bank

When looking at issuing banks, we find that most cards sold by the carding shops have been issued by JPMorgan Chase, with American Express and Bank of America (BofA) taking the third and fourth places, respectively. For unknown reasons, cards issued by FIA Card Services are sold for almost $13.50 each and are generally more expensive than the cards issued by other banks. We also see that `rescator.cm` and `2pac.cc` usually offer more American Express cards than the cards issued by both Wells Fargo and Bank of America combined. The opposite is true for `dumps.pw`, which tends to have more cards issued by Bank of America than almost any other bank. More details can be seen in Table 6.

4.7 Volume and price of cards over time

The average price of cards sold by `rescator.cm` over the past three months was between $9.06 and $17.00 while the cards offered by `dumps.pw` had less variation in their prices ($10.91-$12.89).

When looking at the volume of `rescator.cm` and `dumps.pw` over time, we see that both shops feature periods of relative inactivity followed by a rapid increase in the number of cards available for sale. As can be seen from Figure 1a, which shows the number of unique cards available for sale for both carding shops over a period of the past three months, `dumps.pw` and `rescator.cm` seem to be using different strategies for adding new cards to their shops. The owners of `dumps.pw` usually add less than 3,000 new cards per each update, with every fifth/sixth update containing 6,000+ cards. `rescator.cm`, on the other hand, never makes that many cards available at the same time. Instead, it adds a moderate amount of new cards (1,000-6,000) with each update.

Bank	Total # of cards	Avg. price per card (total)	Avg. price per card (rescator.cm)	Avg. price per card (dumps.pw)	Avg. price per card (2pac.cc)
Chase	18,105	$11.23	$8.71	$13.78	$47.05
Unknown	17,014	$11.21	$9.41	$11.90	$15.19
Amex	11,676	$8.75	$7.96	$9.25	$15.48
BofA	10,673	$10.29	$10.79	$10.07	$19.17
Wells Fargo	7,962	$9.59	$9.16	$9.94	$35.00
Citibank	5,919	$12.27	$9.40	$16.66	$34.64
Capital One	5,033	$12.19	$9.31	$18.81	$43.40
FIA	4,964	$13.37	$7.97	$21.23	$32.84
U.S. Bank	4,602	$9.55	$8.01	$10.93	$15.05
Barclays	1,772	$13.10	$11.23	$13.57	$63.05
Other	45,872	$11.09	$11.37	$10.70	$19.68

Table 6: Card prices by issuing bank

Among the prominent breaches occurring during our data collection included Bebe Stores Inc. and Park-n-Fly, which explains the seemingly never ending supply of cards offered by `rescator.cm` and `dumps.pw`. As can be seen from Table 7, which shows the summary of the most recent breaches, the data breaches are followed by a major update on carding shops' websites (Figure 1a). In cases when the exact time frame of the data breach is unknown, which is true for Park-n-Fly, OneStopParking.com, and Chick-fil-A, the date when the breach was first reported seems to be preceded by a major update on `rescator.cm` and `dumps.pw`.

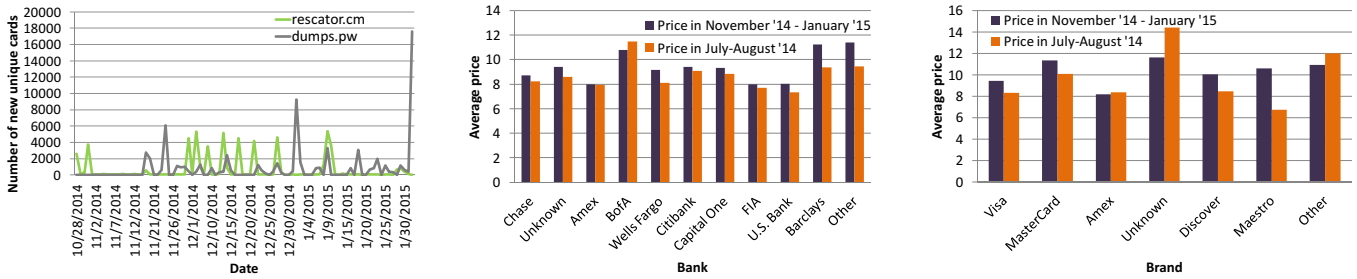
Company	Date of the breach
St. Louis Parking Company	occurred on 10/06/2014 - 10/31/2014 [27]
SP+	occurred on 04/14/2014 - 11/10/2014 [28]
Bebe Stores Inc.	occurred on 11/08/2014 - 11/26/2014 [29]
Park-n-Fly	1st reported on December 16, 2014 [30]
OneStopParking.com	1st reported around December 18, 2014 [31]
Chick-fil-A	1st reported in November 2014 [32]
Book2Park.com	occurred on 10/01/2014 - 01/24/2015 [33]

Table 7: Timeline of recent data breaches

When comparing prices on `rescator.cm` between July-August 2014 and the present, we see that a typical credit/debit card CVV is 33 cents more expensive now than in 2014, while a dump is $3.84 more expensive. One possible explanation for this could be that there have been a large number of high and not-so-high profile data breaches since August 2014, which resulted in more high quality cards available for sale.

When looking at the issuing bank, we see that `rescator.cm` used to offer a significantly higher percentage of Chase cards for sale in July-August 2014 compared to their current inventory. Furthermore, while all other banks' credit and debit cards sell for more now than they used to, cards issued by Bank of America were actually more expensive on `rescator.cm` in 2014 with the average price being almost $1.00 higher compared to 2015 (Figure 1b).

Finally, we observe that American Express is the only major brand that costs less now than it used to last year. In addition, we see that Maestro cards have almost doubled in price on `rescator.cm` over time. One possible explanation for this could be that there were too few American Express cards for sale last year (13.28% of all cards now vs. 1.61% of all cards in July-August 2014), which increased the demand for them, thus, raising the price. More details can be seen in Figure 1c.



(a) Unique cards added to `rescator.cm` and `dumps.pw` in three months

(b) Card banks (`rescator.cm` in 2014 vs. `rescator.cm` now)

(c) Card types (`rescator.cm` in 2014 vs. `rescator.cm` now)

Figure 1: Changes in price and volume of cards on `rescator.cm` and `dumps.pw` over time

5 RELATED WORKS

Although there have been a number of studies on underground marketplaces and detecting and preventing various kinds of fraud, very few of them have analyzed the underground marketplaces involved in selling stolen credit and debit cards. Multiple papers [34–36] propose to use machine learning, data mining, and other methods to detect credit card fraud, but they do not really analyze what actually happens to the credit card once it has been stolen. Others [37, 38] are measurement studies which evaluate and review the existing approaches of detecting credit card fraud.

A 2007 measurement study by Franklin et al. [7] focused on underground marketplaces for credit card fraud, identity theft, spamming, phishing, online credential theft, and the sale of compromised hosts. The depth of focus on credit cards was limited due to the broad nature of the study. Moreover, the paper only used publicly posted IRC messages, which hid transactions that occurred via private messages. Underground black markets have evolved much since that study, with IRC losing popularity among fraudsters. Further, our paper focuses only on credit and debit cards.

A more recent study by Thomas et al. [8] is closer in spirit to our paper. We complement their preliminary work by studying debit cards in addition to credit cards, as well as card dumps and CVVs. Further, we estimate the revenue of underground carding shops, which was not characterized. Finally, our two data collection time periods allow us to draw inferences regarding the debit and credit card prices as well as volume of sales over time.

6 CONCLUSION

In this paper we collect and analyze data from three web-based underground carding shops. We encountered various impediments during and after data collection. The shops regularly went offline for maintenance, updates, and other reasons. They also changed domain names to evade law enforcement. Their hosting was often spotty, with web pages not loading on occasion. Virtually all of them evolved during our data collection to make scraping data difficult: they not only required CAPTCHA solutions before granting access to data but some even required solving CAPTCHAs in the middle of a session. Further, CloudFlare's DDoS protection blocked our scraper from accessing data until we found a way to imitate a real web browser.

In spite of these hurdles, we collected data for two different time periods for a combination of three websites. The analysis offered interesting insights into the financial motivations of miscreants behind these outfits. The lower sale price on about 70% of stolen cards compared to the cost of re-issuing a card suggested that banks might indeed find it cheaper to "buy back" their own cards instead of re-issuing. We found carding websites to be efficient, in that stolen cards are available for purchase soon after a breach. Finally, as the EMV technology takes off in the U.S. to protect against card cloning, our study can serve as a benchmark to estimate its impact on card fraud in the U.S.

REFERENCES

[1] "Anthem Data Breach – 6 Things You Need To Know," http://thehackernews.com/2015/02/anthem-data-breach.html.
[2] "Target: 40 million credit cards compromised," http://goo.gl/gs5i8g.
[3] "The Big Data Breaches of 2014," http://goo.gl/Os7gyr.
[4] "Who's Selling Credit Cards from Target?" http://goo.gl/cjkc0p.
[5] "The Amazon.com of Stolen Credit Cards Makes It All So Easy," http://goo.gl/yOixvm.
[6] S. Corporation, "Symantec Report on the Underground Economy," http://goo.gl/JINjRB, 2008.
[7] J. Franklin *et al.*, "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants," in *ACM Conference on Computer and Communications Security (CCS)*, 2007.
[8] C. Thomas *et al.*, "Analysis of Online Credit Card Black Markets," 2014.
[9] "Recieving Stolen Property," http://goo.gl/6Mm1Vj.
[10] "Debit / Credit Card Fraud," http://goo.gl/qsbxil.
[11] "EMV FAQ," http://www.emv-connection.com/emv-faq/.
[12] "MSR206 Encoder," http://goo.gl/g4Yb0m.
[13] "Dumps vs CVV," http://goo.gl/zqQ1Fa.
[14] "Why So Many Card Breaches?" http://goo.gl/DDu3q3.
[15] "CloudFlare," https://www.cloudflare.com.
[16] "Go digital, reduce fraud," http://goo.gl/mJlPqU.
[17] "EMV Adoption and Its Impact on Fraud Management Worldwide," http://goo.gl/jgVT2W.
[18] S. Drimer *et al.*, "Optimised to fail: Card readers for online banking," in *Financial Cryptography and Data Security*. Springer, 2009.
[19] M. Bond *et al.*, "Chip and Skim: cloning EMV cards with the pre-play attack," in *IEEE Symposium on Security and Privacy (SP)*, 2014.
[20] "More Secure Credit Cards With Chips Coming To The U.S." http://goo.gl/hNycMN.
[21] "Alleged Russian Hacker Faces 40 Charges," http://goo.gl/dh0stQ.
[22] "Seleznev Arrest Explains '2Pac' Downtime," http://goo.gl/3MWNOC.
[23] "Banks have replaced 15.3 million cards since Target breach," http://www.startribune.com/business/242505661.html.
[24] A. B. Association, "Target Breach Impact Survey," http://goo.gl/zXtKNb, 2014.
[25] "Visa vs MasterCard vs American Express," http://goo.gl/WySWY.
[26] "Credit Card/Debit Card Center," http://www.cnbalva.com/cc.php.
[27] "St. Louis Parking Company - Press Release," http://goo.gl/nGNkVa.
[28] "SP+ Acts To Block Payment Card Security Incident," http://goo.gl/QBvNLH.
[29] "Bebe discloses data breach," http://goo.gl/v4TyHl.
[30] "Banks: Park-n-Fly Online Card Breach," http://goo.gl/Uui1lH.
[31] "Target Hackers Hit OneStopParking.com," http://goo.gl/3elS5U.
[32] "Banks: Card Breach at Some Chick-fil-A's," http://goo.gl/IvwSht.
[33] "Possible Data Breach FAQs," http://goo.gl/F1agvj.
[34] R. Brause *et al.*, "Credit Card Fraud Detection by Adaptive Neural Data Mining," *J.W. Goethe-University, Comp. Sc. Dep., Report 7/99*, 1999.
[35] V. R. Ganji and S. N. P. Mannem, "Credit Card Fraud Detection Using Anti-K Nearest Neighbor Algorithm."
[36] M.-J. Kim and T.-S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," in *Intelligent Data Engineering and Automated Learning (IDEAL)*, 2002.
[37] L. Delamaire *et al.*, "Credit card fraud and detection techniques: a review," *Banks and Bank systems*, vol. 4, no. 2, pp. 57–68, 2009.
[38] V. Dheepa *et al.*, "Analysis of Credit Card Fraud Detection Methods," 2009.