The Underground Ecosystem Of Credit Card Frauds

Introduction to Payment Card frauds

Use of Plastic cards as a mode of payment is one of the most widely used and convenient alternatives to cash. This mode of payment is now accessible to the common population of almost all the major geographical locations on our globe. Its ease of use and portability makes it a preferred mode of financial dealing. Such efficiency cannot be achieved without the presence of a large networked ecosystem connected through nodes of various computational devices. But, where there are computers and networks, there are hackers.

Frauds related with Payment cards like Credit and Debit cards have raised serious privacy and authenticity concerns among its users. The recent few years have been worse hit where-in several major retail chains and brands were found to be affected with such frauds. The high monetary profit involved in this theft has attracted the biggest online cybercriminals and hackers to build their own empire with tightly knitted gang of individuals and groups. Most of the major payment card frauds are financially motivated and spans over several months starting from stealing the user information to conducting actual frauds. This paper goes into the details of how this entire fraud ecosystem functions and how it is disrupting the current electronic payment industry at a large scale.

To start with, let us first give a quick read at some of the key vocabularies that will be used throughout this paper and will be relevant in further understating the key discussion points.

Key Vocabularies

Credit/Debit card: A monetary instrument, often referred to as plastic cash, used to make payment for goods purchased. A Debit card is linked with the user's bank account and can be used to purchase goods worth value not exceeding the amount of money in the linked account. A Credit card is a temporary loan purchase; where-in the bank pays for the purchase value and recovers the cost from the user later on. Credit cards also have specific monetary limit.

PIN (Personal Identification Number): A personal numeric value used to validate the card owner.

CVV/CVV2: 3 or 4 digit number printed on the card. This number is used as an additional verification point to validate the cardholder.

BIN (Bank Identification Number): The first six numbers of the card that is used to identify the issuing bank and in certain cases, the type of card.

Card brands: Refers to the authorized companies whose network is used to facilitate the interaction between acquirer and issuer. Popular brands include Visa, Mastercard and American Express (Amex). A card starting with a 4 is a Visa, with a 5 is a Mastercard and with a 3 (15 digits long) is an Amex. A comprehensive list is provided later in the paper.

Buyer/Consumer: The cardholder who purchases the goods and uses card for payments.

Merchant: Goods and service provider who accepts cards as a mode of payment.

Acquirer Bank: The bank responsible for processing the merchant's credit card transactions with the buyer.

Issuer Bank: The bank that issues credit card to the consumer.

POS (Point Of Sale): POS machines are the card reading devices used to carry out the monetary transaction between the buyer and merchant.

Magnetic Strip: The black strip on the backside of the credit/debit card that stores various details required during financial transaction.

Tracks: Information on the magnetic strip is saved on tracks 1,2 and 3. The first two tracks are generally used to store the details like account number, owner name etc. The 3rd track is optional and used for storing additional data.

Card dumps: The raw un-encrypted data extracted from the temporary storage(RAM) of POS devices. These dumps carry information written on tracks 1 and 2 that are read by the POS device while making transactions.

Card reader/Writer: Is a piece of hardware and software that is used to write data onto the magnetic strip of the plastic card. MSR-206 is the most popular encoder used for writing data over cards.

Carder: Is the individual who uses the stolen plastic card information to carry out fraudulent transactions.

Runner: The individual/group who uses the counterfeit cards to cash out from ATMs.

Dropper: The drop point for goods purchased online. The Dropper is usually an individual whose sole purpose is to receive the ordered item and deliver to the carder in return for cash or other goods.

Shopper: Is the individual/group that does in-store shopping with counterfeit cards. These shoppers also carry fake IDs to make the fraud look more legitimate. Usually the carder can himself be a shopper or a runner.

EMV: EMV or Chip-and-Pin cards are an alternative solution to swipe cards, which stores data on a chip in an encrypted manner. Even though the storage mechanism is encrypted, POS based malwares can still steal the data once it is decrypted in the memory.

Contactless RFID cards: Another enhancement to traditional magnetic strip based cards. In RFID enabled cards, the buyer can pay for the goods by simply waving the card close to the POS terminal.

How Credit Card payments are processed

Credit card transaction involves several steps before the payment is finalized. Here are the main steps involved during a transaction using credit card:

- *Authorization*: Cardholders request to purchase goods from using his credit card. The merchant submits transaction requests to acquirers. Acquirer then sends the transaction requests via cardholders' card brand network to issuers. Issuer returns authorization codes via card brands' networks to acquirers. Acquirers then forward authorization codes to merchant. If the transactions are authorized, merchants give cardholders the goods or service as requested.

- *Batching*: Merchants store an entire day's authorized sales in a batch. At the end of the day, they send the batch via payment service providers to acquirers in order to receive payment.

- *Clearing*: Acquirers send the batch via card brands' networks to issuers in order to request payment. Card brands' networks sort out each transaction to the right cardholders. Issuers then transfer requested funds via card brands' networks to acquirers.

- *Funding***:** Acquirer sends the payment to the merchant via the payment service provider. The payment is then billed and the amount is paid to the merchant.

These steps are just an outline of how the payments are processed using credit cards. There are several other authorization steps involved as well, but these four points form the major building block of the transaction phases.

Now that we have a fair amount of understanding about the Plastic card payment system and how things are related, we can now move towards more technical details like the stolen dumps, the steps involved in fraud transactions, identifying weak points etc. But before that, let us give a quick look at some of the common entry points used by the hackers in order to exfiltrate critical payment data.

Types of Thefts

Any credit card related theft involves following three steps:

- Reconnaissance
- Attack
- Sell

The financially motivated actor first studies the attack environment and tries to identify the weak points (Recon) that can be leveraged to craft an attack vector.

Once the weak points are identified, the attack phase begins. The main attack techniques include:

- Key logging
- Phishing
- Vulnerability Exploitation
- POS memory scrapping malware

Out of all these techniques, POS memory scrapping is the most widely implemented attack vector. The reason being it directly affects the device/medium that is used as a primary processing device for card based payment systems.

The point to note here is that, there has to be a delivery medium by which the POS malware gets introduced into the system. Phishing and vulnerability exploitation are the two popular ways of setting up a delivery mechanism for POS malwares. Insider threat has also been a key factor in infecting POS terminals.
We will discuss POS malwares in brief here, as it is currently the talking point of this fraud ecosystem. It is the main weapon that is empowering the cybercriminals in targeting one of the biggest retail chains and brands across different regions.

POS malwares in a nutshell

Point of Sale or POS terminals are the main processing devices between the buyer and seller when a card based payment system is involved.
POS based malwares are special purpose malware/virus program that are designed to scrape data from the terminal's main memory. The idea is to steal the unencrypted data that gets copied to the terminal's primary memory (RAM) when a credit or debit card is supplied to it for payment processing.

There is a slight misconception about POS devices that the data is sent to and fro in an encrypted manner. This is certainly true, but there is a short period of time when the POS terminal reads the data from cards and is stored in plain text manner in its primary memory before it gets encrypted again. This is where POS malwares comes into action and scrape the information from the memory.

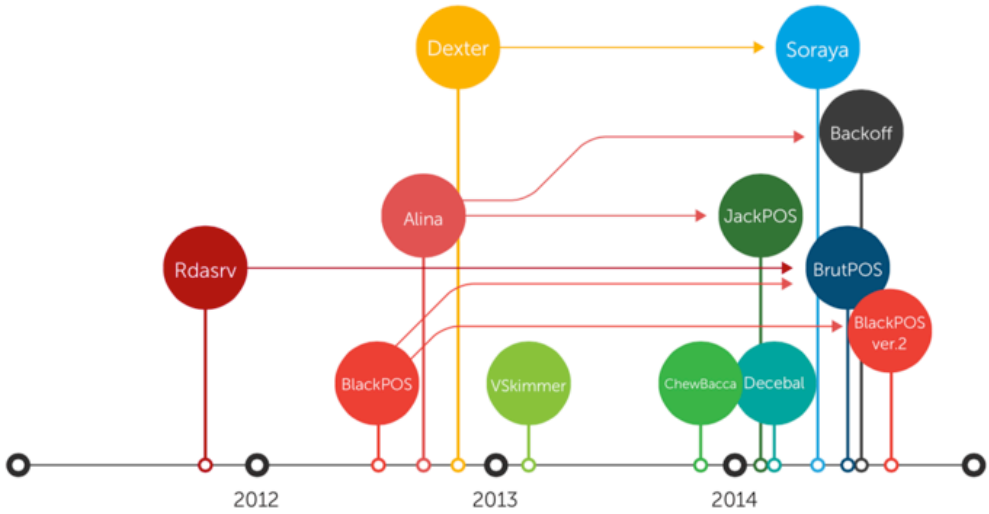

Figure 1: POS Malware Family chart. Image source: Trend Micro

A detailed discussion about the technical aspects of POS malwares is beyond the scope of this paper. Here I will summarize some of the key features/steps of this malware family that makes it a lethal weapon against plastic card based frauds:

- POS malwares include all the basic functionalities of a malware like data exfiltration using networks, collecting system information, communicating with its command and control servers, kill switch to remove themselves from the infected system etc.

- They have a specific purpose of scraping terminal's memory and reading card data.

- They achieve this by first reading all the processes loaded into the device memory. They keep matching the running process names against their own local database to figure out which processes to scrape and which process to exclude.

- Once the processes are figured out, they can either execute custom functions or specific regular expressions in order to read data from the memory that matches with credit card information (Track 1 and 2 information).

- Once the data is scraped from memory, it is written onto the disk and stored at a specific location. Once the malware finds a live network connection on the terminal, and its parent controller is reachable(C&C server), it transfers that written file to its server (can be encrypted or un-encrypted) thus successfully exfiltrating the data.

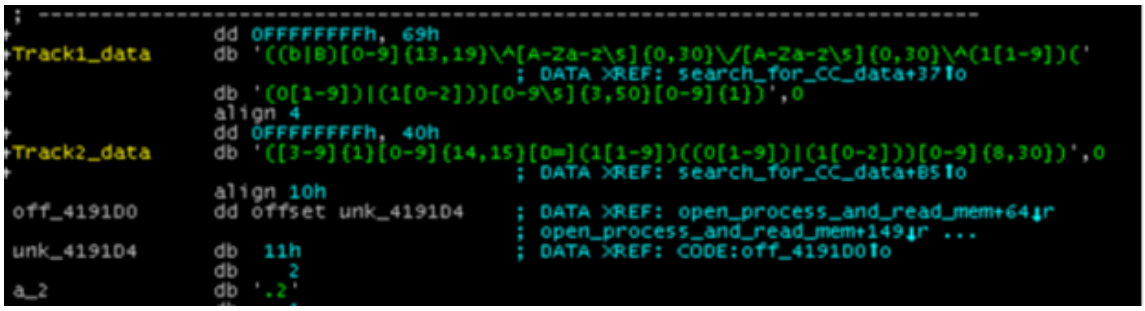

Figure 2: POS malware using Regular expression to match credit card data in memory

Understanding the POS dump data

Now that we have built up a background on how the POS terminals are infected and how the data is stolen, we can now have a brief overview of the data that POS malwares steal, how it looks like and how it is intercepted.

Here is an example of cleaned up data sent by a POS malware to its C&C server:

Track 1: B4096654104697113^ABHINAV/SINGH^0806101273590052100000 0

Track 2: 361344212572004=0512052335136; ABHINAV/SINGH

Track2 + Track1: 4411037117155348=14111010000013500000; B4411037117155348^ABHINAV/SINGH^14111010000000135000000?

165430 | 134884 | 2 | 4921817934747226 | 4 | 2008 | 3 | 2010 | | 662 | ABHINAV SINGH | 10 | VARUNA APP | VARANASI | PO139UX

468442/ 165337 | 134815 | 2 | 4921817809597243 | 3 | 2008 | 2 | 2010 | | 185 | ABHINAV SINGH | 10 | VARUNA | VARANASI | PR4 3HB | | lancs 01436672207

This looks like some random series of data dumped by the malware, but it is not. In order to make sense of this data, let us first spend few minutes on the structure of magnetic strip and the format in which it stores data on various tracks.

Track 1 and 2 Block Diagram

Magnetic strips are logically divided into tracks or records that is used for storing the data required during financial transaction. The logical placement is shown in the following diagram:

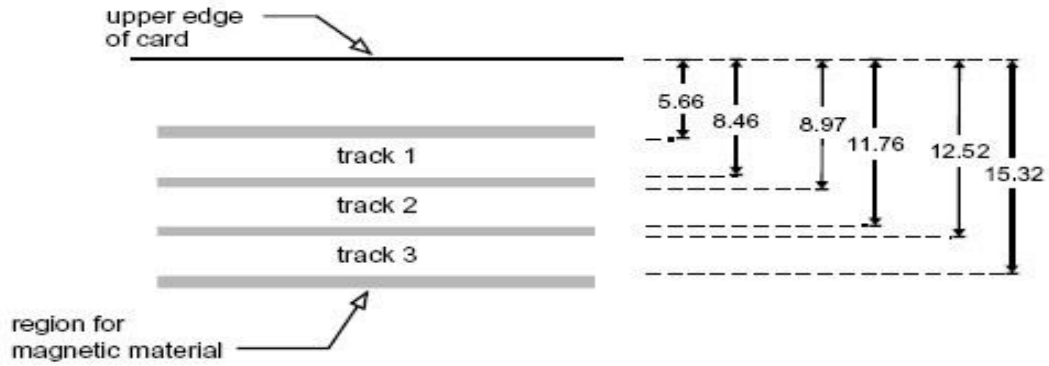

Figure 3: Logical placement of Tracks on Magnetic strip

Tracks are placed in a sequential order where Track 1 is followed by Track 2 and 3. The reading of data also follows the same order.

Track 1 and 2 are mostly used for storing crucial data. Track 3 is used for storing optional data. Depending on the banks choice, they can either store financial details either on Track 1 or Track 2. Both these tracks follow specific format for storing the data. Let us give a quick look at the block diagram of both these tracks to understand the format in which the data is stored and read on these tracks:

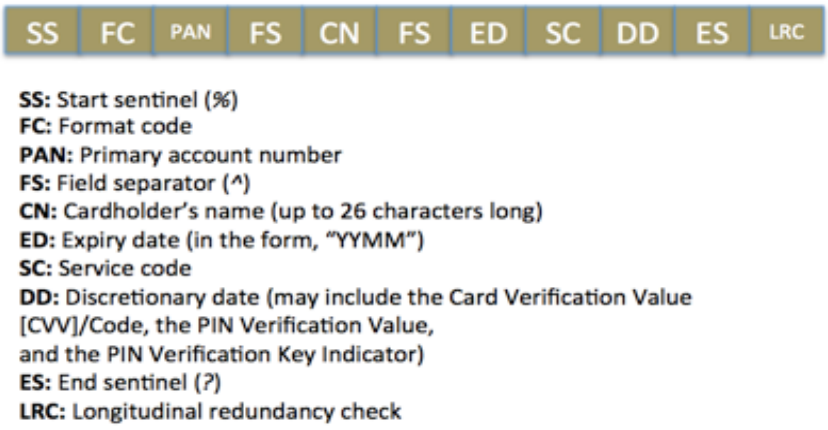

Figure 4: Track 1 block diagram

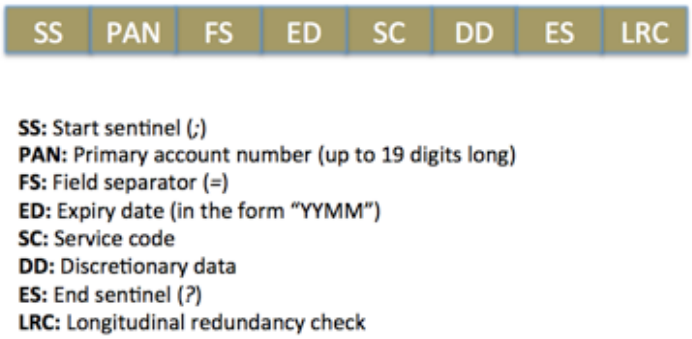

Figure 5: Track 2 block diagram

Both Track 1 and 2 store information in blocks where each block represents specific value, each having a particular storage limit and separated by delimiters.

Let us take the example of track 1 data dump once again and analyze it based on the fields we learnt in the block diagram:

Track 1: B4096654104697113^ABHINAV/SINGH ^0806101273590052100000?

Consider no values for SS and FC, The first seventeen characters represent the Bank Account number (B4096654104697113) followed by the field separator (^) and Account holder's name (ABHINAV/SINGH). The next four characters represent expiry duration of the card in YYMM format (0806). The next few digits follows are the Service code (1012735900) and Identification number (521). The next few digits are the filers for the remaining bytes.
Similarly we can also read the Track 2 data.

The point to note here is that Track 1 data is sufficient information when dealing with card dumps. It contains enough information to be converted into Track 2 dump as well. There are online tools available as well to do the conversion with ease. ***Trackgenerator.net*** is one such online service. Most of the online carding forums sell track 2 data.

To quickly summarize our learning so far: we have seen how the plastic payment networks work. Then we read about the different threats that posses to these electronic payments. We then emphasized on POS malwares and their behavior. Then we saw what kind of information these malware steal. Now we will move to our actual agenda: How this stolen information forms the crux of an ever-profitable cyber crime.

The Underground Shopping Mall

Now that we have built enough background into understanding the Card payment system and the threat associated with it, we can now move to our agenda, which is to understand how this stolen data is converted into a profitable cybercrime network.

There are three major steps involved in building a complete cybercrime ecosystem for credit card frauds. These are:

- Attack
- Sell
- Shop

We have already seen in detail how malware authors and hackers craft various attack vectors in order to steal payment critical customer data.
Now we will move to the second step, which is to set up a shopping mall for the stolen data.

Carding Forums

Carding forums (popular name) or dedicated websites for selling credit and debit card data are the most popular means of connecting with the mass newbie and elite group of people who have adopted this fraud as their full time profession. These forums are pretty similar in design and format, but what sets them apart is their source of dumps.
For Eg, a popular underground forum ***rescator.su***, came into limelight when it was linked with selling dumps stolen from Target retail store breach (source: krebsonsecurity.com). Overnight, this store was flooded with tones of data. In my sequence of following this forum for couple of months, I noticed some key changes in their selling model, which was a result of customer complains and process improvement. The forum was re-designed to include couple of selection options for its buyers:

- Initially the dumps were only classified based on their brands like Visa, Mastercard, Amex etc.

- Later on additional filters were added like, dumps with specific details or belonging to a particular country. Dumps with Signature and Platinum stature were certainly costlier than others.

- Later on, the city to which the details belong also became critical. So it was added as a filter criterion.

- Banks and Payment networks continuously monitor payment transactions to detect fraud. Hence, oversea usage or out of city usage of card without notifying the banks was one trigger point. This is where buying dumps belonging to a particular country and city plays an important role.

- Later on an interesting feature was added which rates the success rate of a given card detail. This rating is based on factors like how old is the dump, how close it is to its expiry date, cards stature (platinum, titanium etc.). The CC details with lower success rate were relatively cheaper compared to those with higher success rate.

Later on, these specifications and improvements were copied over by other carding forums as well. Multiple shops started spawning in a short period of time. Some dumps were tracked back to its seller forums in order to identify their sources and some went undisclosed. Last couple of years has seen an exponential rise in both sellers and buyers of carding frauds.

Buyers

Once the stolen card details are up for sale, the paddle starts rolling. The next entity that comes into picture is the buyers of these stolen details. Here are some key highlights from the role a buyer plays in this ecosystem:

- The buyer profiles of these forums include newbies as well as experienced and regular customers. Both Buyer and seller gain more and more reputation based on their loyalty and frequent engagement.

- Buyer has the option to buy either single card detail or a group/collection of multiple unsorted details called dumps. There is another category called "Fullz". This consists of cards with complete details like CVV, Country, City etc.

- The buyer can also leverage the various form filters mentioned earlier (card brand, country city etc.) in order to choose credit cards of their interest. For example, a fraudster living in Singapore would prefer buying dumps from Singapore or Asian region to avoid automatic blockage of overseas usage.

- The buyer can pay to the seller using crypto currencies, bitcoin being the most popular one. This gives additional anonymity to the face behind selling dumps.

- The price of cards and dumps completely depend on the freshness and genre. On an average, a single Mastercard or Visa platinum card will range between $15 to $50. Buying dumps is relatively cheaper as it is a bulk purchase. Dumps price varies between $50 to $200 and contains on an average 10 card details. A bulk purchase of multiple dumps would cost between $600 to $5000 depending on the quantity and quality.

- The download link to the dumps or card details is usually provided over a TOR based onion routing network to make sure that the location cannot be tracked back. IRC channels are also used actively for this purpose.

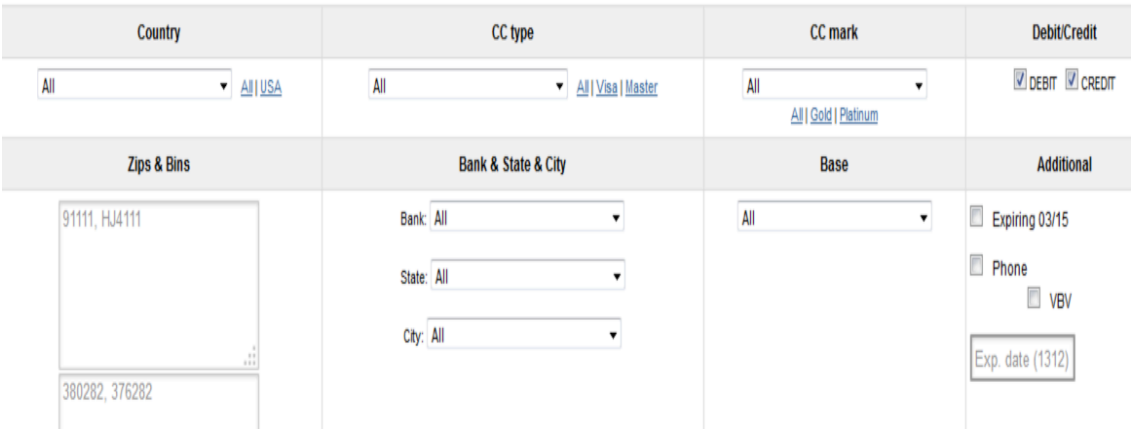

Figure 6: Different selection options for Buyers. Image source: Rescator.so

This is how the buyer gets introduced into this ecosystem and from here on, the buyer is the main driving element of the entire fraud ecosystem. Now the big question comes up is what would buyer do with the raw dumps supplied by the seller. The buyer now has two distinct options:

- Online Carding
- Offline/In-store Carding

Let us know more about each in detail.

Online Carding

Online carding is the process of using the stolen credit card details for purchasing goods online. This step involves some pre-steps before the buyer can go online and use the purchased card details for shopping. The first and the foremost important thing is knowing the CVV number. Most carding forums usually sell CVV details as well along with the card details. In case the CVV is not present, the buyer will have to follow some additional steps in order to obtain CVV number from the original owner of the card. These steps might include Phone phishing; fake postal mails asking for card verification etc. Buying "Fullz" is the most preferred option for online carding as It has all the required details.

Once the CVV is available to the buyer, he now needs to figure out *cardable websites*.
Cardable websites are those website that meet the following criteria:

1. Making sure that the website's terms and conditions do not specifically ship items only to the card's registered address. It should ship to other shipping address mentioned during purchase as well.

2. Making sure that International shipping is allowed.

3. The next thing to look for is weather the website has Visa verification code or Mastercard secure code enabled. This is a two-step authentication where the payment gateway asks for a secure code before proceeding with payment. The card owner only knows this secure code.

4. Check for additional security measures like card scans, delivery at door even when there is no one home, call backs to confirm item payment etc.

It is not easy to find such websites but professional fraudsters are good at finding work around. Several Gambling and online casino websites usually don't have such strong security measures thus giving a good scope for fraudsters to add money to their gambling account. Buying porn website subscriptions, buying crypto currency, online betting and gaming are few other popular ways of using CC for online carding. Underground forums are a good place for finding new and updated list of cardable websites. The community is tightly knitted and carders keep posting their findings into these forums to make sure that the ecosystem is ticking.

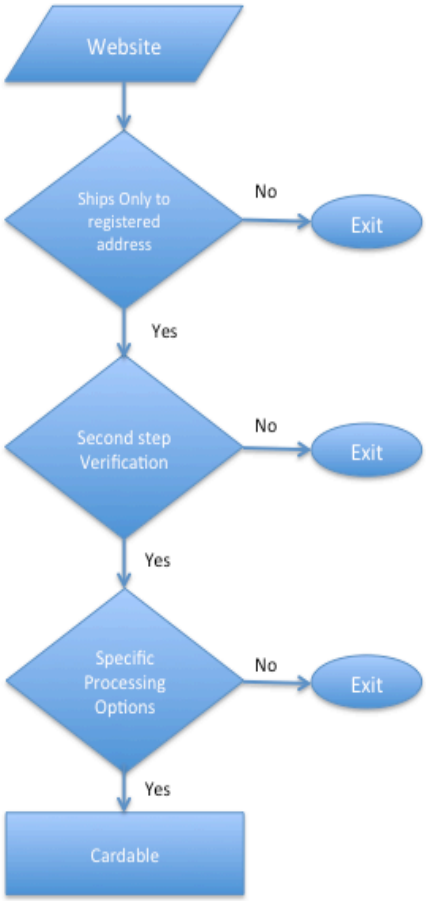

Figure 7: Flowchart for finding a cardable website

Offline/In-store Carding

Offline carding or in-store carding is far more interesting and involves a much larger group to perform it successfully. As its name suggests, offline or in-store carding means swiping the counterfeit cards at the actual stores or POS terminals to make purchases. In order to this, the buyer must convert his dumps into plastic cards. The buyer can either do it himself if he has the required hardware and software or he can again head back to his darkweb to let third party do this for him. There are specific stores in the darkweb forums that specialize in creating counterfeit cards using the dump data. They provide wide verity of options based on card brands, genre etc. Their neatness and enhanced customization make them a vital part of this fraud ecosystem. But at times, there are chances of a double fraud where the fake card generating store might run away with your dump details thus leaving you with nothing. Reputation is the key to this fraud system.

Many professional carders prefer generating counterfeit cards in-house to avoid leakage of their purchased dumps. In order to do this, there are some specific hardware and software requirements.

- Plain plastic cards or fake counterfeit cards without any data on magnetic strip.
- Magnetic card reader/writer.
- Software to write Track 1, 2 and 3 data onto the plastic cards.

Figure 8: MSR 206 with Plastic cards

Briefly, following steps are involved in generating counterfeit cards using the above mentioned requirements and purchased CC details:

- The process begins by purchasing the counterfeit cards or plain plastic cards with magnetic strips.
- Once the card is available, the carder now requires a combination of Encoder hardware and software to write data onto the magnetic strip.

There are multiple variants of hardware available readily on popular e-commence websites and underground hacking forums. The most popular encoder amongst the community is the MSR206. It works fine with most versions of OS and compatible with popular encoding softwares like "thejerm" and "Exeba".

- The process of writing data to Magnetic strip is very much self-explanatory. The carder needs to provide Track1 or Track 2 or both the track information from the dumps into the encoder software.

- Once the software is provided with these details, the hardware needs to be set up and the card needs to be properly placed in the encoder hardware. Once the writing process is complete, the card is now reading for shopping.

There are some additional precautionary steps taken by carders for example:

- Generating fake signature at the back of the card for verification.

- Generating fake ID. In case of large purchases, the shop might ask for a valid ID proof before accepting the card.

- Having backup cards or cash in case the presented card payment fails. This would make the purchase look genuine to the merchant.

Offline or in-store carding may sound a bit risky but it has better success rate compared to online carding. Swipe and use is a convenient mode of payment for the merchants as well so they usually do-not look at such card usage as suspicious. On the contrary, online shopping involves computer based authentication and authorization so the chances of failure are high.

Carders also keep an eye on finding out ways for a more risk-free offline carding. Some of the most discussed and widely used techniques include:

- Using the card at self-service gas stations or self-service grocery stores. Usually there is no payment machine supervisor present at the self-service payments and the carder can easily swipe even a white plastic card and make the payment.

- Choosing stores that do-not have enough security measures like CCTV camera or the supervisor is not very active in checking the card and ID before payment.

- Making sure that they are dressed properly if purchasing some expensive or luxury item.

Specialized Services in the Fraud Ecosystem

Now that we have understood the most critical parts of plastic cards based payment system, there are some other important aspects of this ecosystem that involves specialized services for carders. These specialized services reduce the overall burden of running the entire process single-handedly. Individuals and groups providing these specialized services usually work as partners with carders and form a close-circled group to run the entire business model. The profit is shared between them based on the role everyone plays. The three most important specialized services are:

- Runners
- Droppers
- Shoppers

Runners

Runners are the risk bearers who are on a running spree for making fraudulent transactions from counterfeit cards obtained from carders. Usually card owners have messaging/email services activated where-in the bank sends a notification message or email for any transaction made on their cards. This might alert the card owner that a fraud transaction has been made and he can request the bank to block his credit or debit card.
This is where “Runners” specialized service comes into account. Runner is usually an individual or group whose sole purpose is to make as many fraud transactions as possible in a limited amount of time. Their prime target is doing ATM withdrawals as it provides hard cash for immediate use. Runners often generate multiple fake debit cards for same detail in order to make multiple withdrawals from different locations at the same time. Card details stolen from ATM skimming are the main focus of Runners, as its information is fresh and live as well as it can provide hard cash from withdrawals.
There is another service that a Runner can provide, that involves lesser amount of risk. That service is having Fake accounts on Payment service providers like Paypal, Western Union, Ucash etc. The Runners are capable of creating multiple fake accounts with these payment services, and the buyer uses these accounts to transfer funds directly into these fake accounts. Paypal and Western Union are the most commonly used services for such frauds. Once the payment reaches the fake accounts, the Runner starts withdrawing funds or can safely transfer it to Buyers account by following the shield of multiple transfers.
Runners also hold fake bank accounts in different countries and use them to withdraw cash sent using stolen cards.

Runners are the risk bearers; hence their profit margin is also high. They usually charge the carder between 40 to 60 percent of the money stolen in a single run.

Droppers

Dropper is another interesting specialized service popular in credit card fraud business. Let us say the carder wants to do some online shopping form the dumps he purchased and he wants to buy some expensive luxury stuff. He has the card details for payment, but he also needs a shipping address that can't be traced back to him. Droppers came out to be the business solution for this problem.
The Dropper works in various ways. Once of the easiest ways is to rent an apartment for a month or couple of weeks. Dropper provides fake details in the tenancy agreements using his fake IDs so that his tracks are clear. The Dropper now has an address where the carder can ship his item.

The Dropper may consult with multiple carders and provide them the address details so that he can make maximum return out of his effort. Droppers may also span across different countries to facilitate overseas shopping for the carder. Once the Dropper has received all the items sent by the carder, he can then move out of his rented apartment before the fraud delivery could be tracked back to him.
There are some Droppers who also rent out PO Box numbers using their Fake or expired IDs in order to receive the goods in their registered PO Box.
Since the Dropper bares a fair amount of risk, his profit percent varies between 30 to 50 percent. In certain situations the Dropper might request for a product order of his choice in return for the ordered good for the carder.

Shopper

Shopper specializes in shopping with the counterfeit cards provide by the carder. The Shopper can be an individual or a group that specializes in conducting nervousness-free shopping of goods using the fake cards. This is an important aspect because shaky hands or sweaty face might raise suspicion while shopping with fake cards. The shoppers also have Fail-safe techniques to doge the payment supervisor in case the card fails to authenticate. Shoppers is the most in-demand service of this fraud ecosystem as it involves lesser risk compared to other services and the carder can pay a small profit cut in the range of 10 to 20 percent in return for the shopped goods.
The profit margin for Shoppers depends on the type of good the carder wants them to purchase. Expensive luxury items would require a larger profit share to be paid to the shopper.

The point to note here is the organized way in which this entire fraud ecosystem has been built up. The high profit margin and scope of evasions has attracted almost all the major cyber criminals into this ecosystem.
This kind of balanced and optimized model is not set up overnight. It involves a series of progression and development. Whatever we just now learnt is not new. This payment fraud ecosystem has existed for years under our nose and it still continues to foster. In the closing few pages, I would like to discuss about the

Economics involved in this fraud ecosystem, its challenges and possible solutions in order to remediate these threats.

Money Flow

This entire fraud ecosystem is motivated by financial gains hence money is an important factor in this system. We already have a fair amount of understanding of how the stolen details are pushed to online shops and how the fraudsters are using it to conduct fraud. Let us revise the entire flow again and add the financial instance to the entire process.

The top of the pyramid comprises of the originators or the creators of the attack vector. They include POS malware authors, phishing attackers, insider threats etc. At the beginning of the stage, there is not enough investment or return involved in terms of money. The attackers spend their resources and time into crafting the perfect attack vector in order to gain privileged access.
Once the attack is successful, the attackers start listening to the incoming data to find something meaningful out of it. Once they have their wealth of information, they begin cashing on their hard work.
The attackers have two options: to either set up their own shop or reach out to an already reputed carding shop in the underground network that has trusted customer base.
Based on the amount of credit card data that the attackers have to offer, they reach to a settlement with the forum owners for a fixed amount of money. This is the point where money gets added into this ecosystem. Now a significant amount money has been invested by the card forum owners, they would look to make return over their investments.
Before releasing the dumps for the public to buy, the forum owners first reach out to their trusted circle of carders who work full time into this business. The reason they do this is because a silent release of dumps will give their trusted circles an upper hand into quickly making profit and they would be willing to pay a descent amount for getting an upper hand at a fresh set of dumps.
Once the dump is brought up for sale, the demand goes high and there is a sudden flow of money in the network. Newbies and other regular carders start making bulk purchases. Taking quick action is also a key factor in the carding business because dumps might have limited availability and once the dumps are made available for purchase, the banks can track back the infected merchant and can quickly block all the cards that were used at that merchant store in a particular range of time. Banks and financial institutions will waste no time in doing damage control. By the time the dumps get old or there is a press release regarding the source of the dump, the forum owners and sellers would have made their profits. When dumps are released for sale in millions, there is not enough that the banks and financial institutions can do. They can trace back a few cards but not all.

Since the dumps are already ported onto counterfeit cards, the wheel starts rolling and the seller who has made investment will now start making his return with the help of runners, droppers and shoppers. They will in-turn get their share of profit.

Once the seller has recovered his investment and started making profits, he will again head back to the forums and shops to continue the cycle.

Demand and Supply

In the recent couple of years, POS malwares have proved to be the most effective means of stealing payment card information. The reason being they directly affects the device that is associated with the payment, the POS terminal. Installing POS malwares and mega retail chains and big brands resulted into millions of credit and debit card data hanging out there for people to buy and conduct financial fraud.

As soon as there is a hint of a major POS breach, the carding community gets active to quickly get their hands on the most fresh and reliable dumps available in the market. This leads to a sudden raise in the demand for dumps especially in the areas where the POS terminals are affected. For example, A press release about a major POS breach in US would lead to a higher demand for fresh dumps in that region. The card shop owners try to make sure that they are able to maintain a good flow of dumps at regular interval so as to meet the demands.

But the problem occurs when the supply is way more than the demand. At times, eminent researchers and financial institutions are able to identify a major POS breach even before the dumps are released in underground shops. The forum owners and sellers might be in possession of those dumps captured from the infected terminals but they have not yet publically released it for sale due to various factors. But when there is a press release about the breach, then the banks and general public will become aware of it and thus the dumps might lose its value if stays unused for long. So in order to make some profit over their investments, the shop owners and sellers quickly release the dumps for sale. Usually these dumps are released in bulk figures (thousands, millions etc) thus making a surplus presence of stolen card details in the market. This is the situation where the supply might surpass demand. So to keep up the momentum, the shop owners and sellers begin lowering the price of their dumps and cards. This brings down the market valuation thus creating deficit.

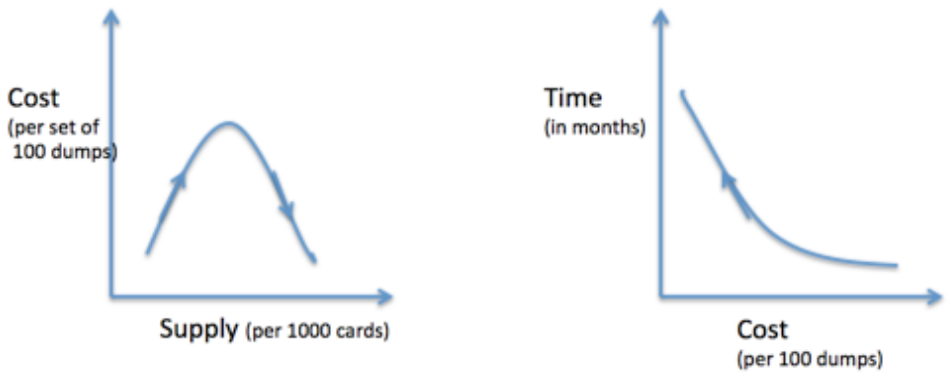

Figure 9: Supply/Cost and Time/Cost Graph

The following two graphs explain the logic. When the supply is moderate and as per the demand, the price is higher than market value but when there is a surplus supply and the demand is stagnant, it leads to a saturation point and thus the price starts falling thus forming an inverted parabolic curve.

Similar results are seen in the plot for Price versus Time. The longer a dump stays in the market, the lesser will be its value thus further lowering its demand.

Credit Card fraud Ecosystem in a Nutshell

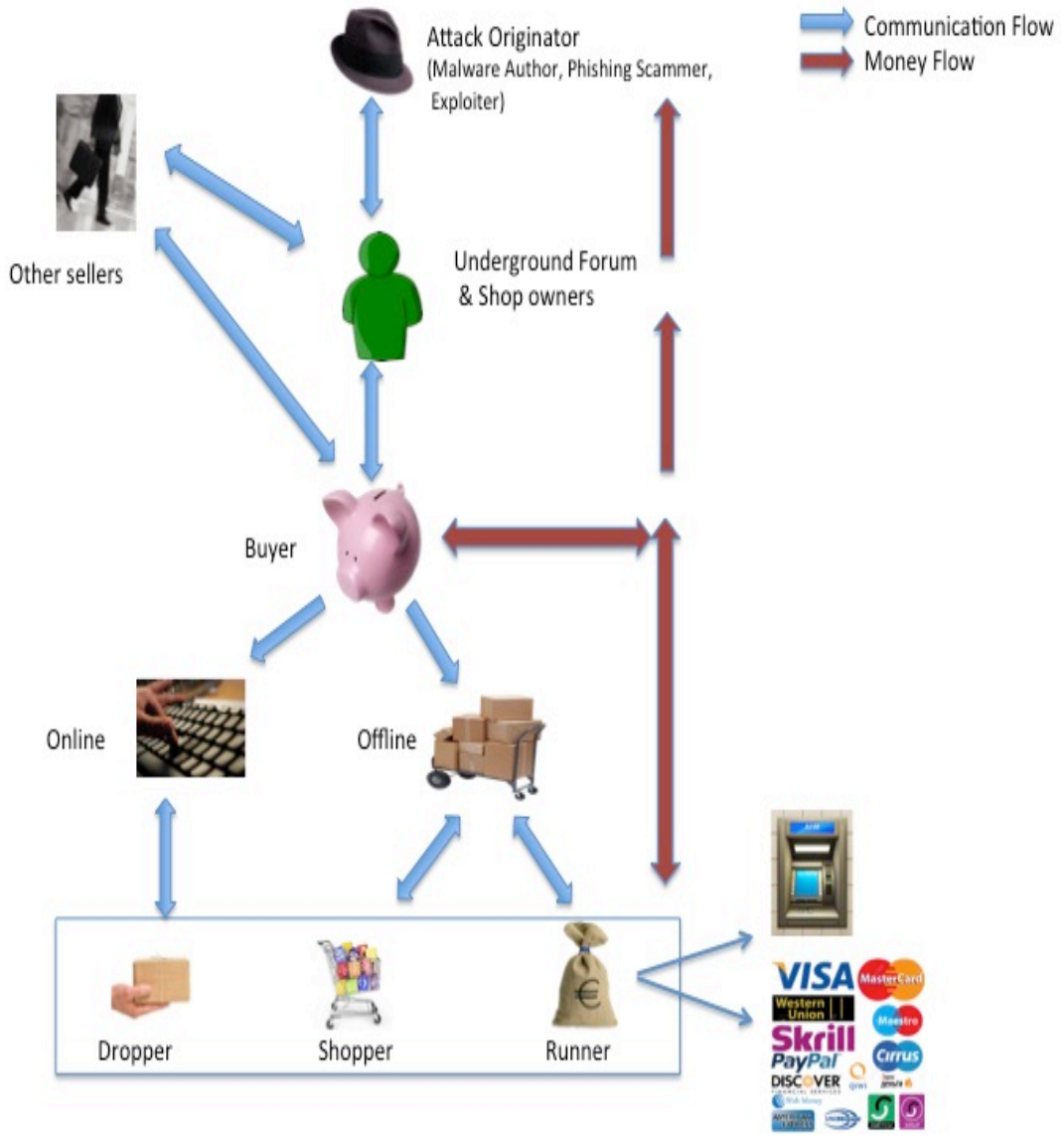

Figure 10: Credit Card Fraud Ecosystem

Future Scope, Challenges and Solutions

Credit card fraud has been around for years now and with time, the model has grown stronger and better with each passing day. More and more criminals are getting attracted towards it thus leading to formation of a new kind of underground mafia group. As more and more newbies and computer expert yet unemployed people gets attracted towards this model, it will continue to grow at the same pace.

The major challenge that this ecosystem faces is double fraud, ie, fraud within fraud. Many times, the buyer purchases the dumps, uses it and once it is blocked, they again put it for sale onto different forums. Also there are fake sellers whose main motive is to attract buyers and in-retrun rips them of their money. There is no way to verify the originality of dumps in advance. Since most of these dealings are in crypto currencies, they can't be tracked back easily. Reputation plays a key role here. Sellers and buyers with good reputation are trusted more compared to a new or unknown seller. Some other challenges include controlling the abuse, keeping the operation stealth, avoiding being caught etc.

The payment industry has been dealing with this issue seriously but the problem lies in the widespread reach of card usage. It is not easy for them as well to enforce certain changes in a go.
EMV or Chip-and-Pin cards have been introduced as a new replacement for Magnetic strips. The EMV card stores information on a chip in an encrypted manner thus making it difficult to skim the information. EMV cards are also difficult to counterfeit, as faking a chip on top of the card wont be easy. But EMV cards are still susceptible to POS memory scraping.
Introduction of Contactless RFID cards are also the talking point these days. It allows the card owner to just wave the card in front of the POS terminal in order to complete the payment transaction. Both EMV and RFID have their own set of protocols and security measures defined in a definite manner to insure maximum security of the customer.

To conclude, this has proven to be yet another cat and mouse battle where the mouse has always been a step ahead. Cybercriminals are always looking for new ways to make easy money by exploiting the weaknesses that they are always ahead in finding. Bob Russo, General Manager of Payment Card Industry Security Standards Council says, "There is no single answer to securing payment card data". Certainly, building a 100% secure model is not possible, but progressive steps and learning from previous mistakes can atleast make things more difficult and challenging for the criminals from stealing the hard earned money of the common man.