The Underground Ecosystem Of Credit Card Frauds

Abhinav Singh

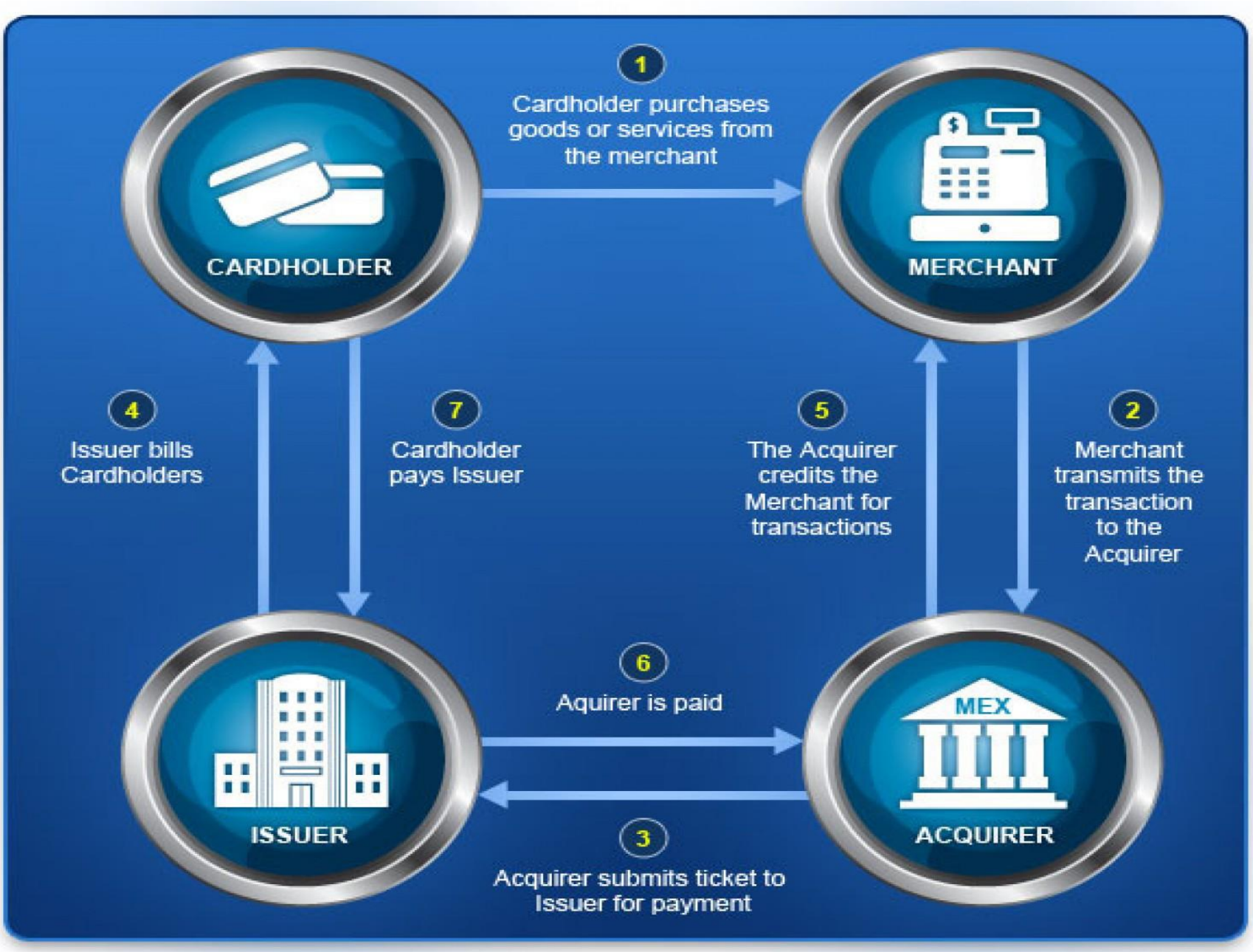
@abhinavbom

#malwaremustdie

Agenda

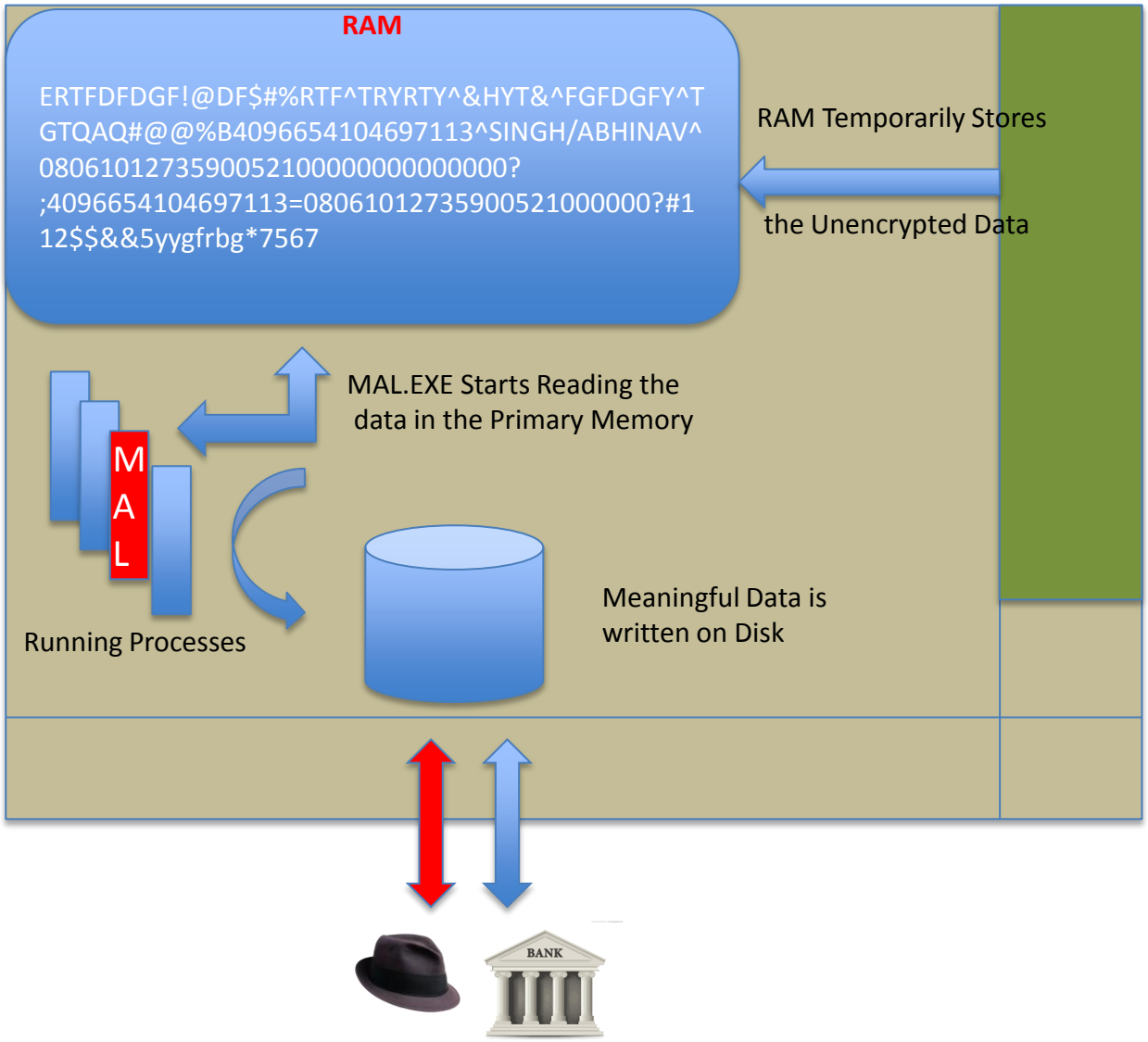
- Brief Introduction to Card based Payment Systems.
- POS Malwares and the Data dumps.
- Understanding the Underground Shopping Mall.
- Money flow, Demand & Supply
- Future Scope, Challenges & Solutions

Processing Card Payments



Key Components

POS RAM Scrapping Malware In a Nutshell



Dumped Data

%B4096654104697113^SINGH/ABHINAV^
0806101273590052100000000000000?

;4096654104697113=080610127359005210000000?

Inside the Plastic Card

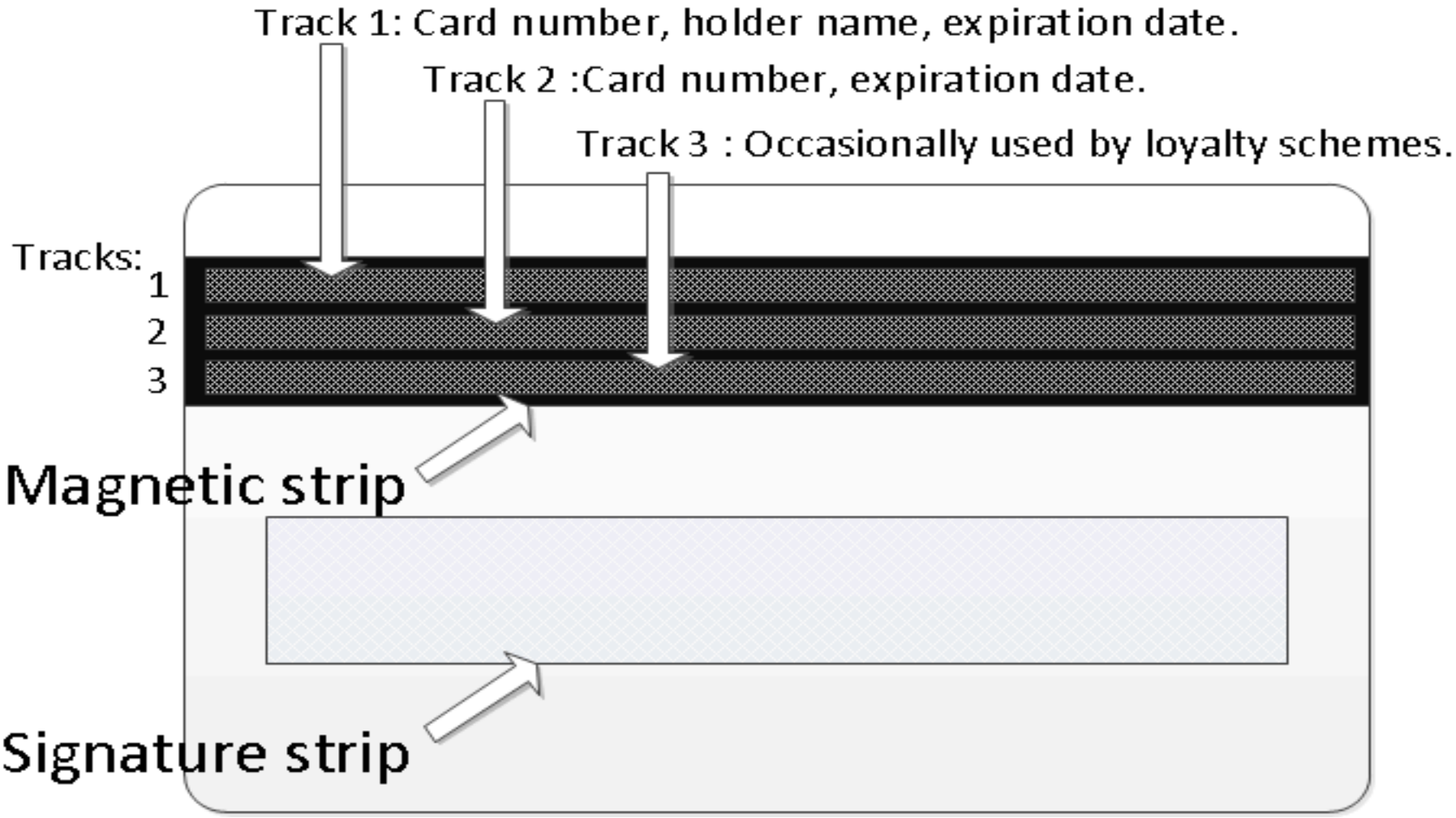


Image source: Blog.cisco.com

Track 1 & 2 Block Diagram

%B4096654104697113^SINGH/ABHINAV^0806101273590052100000000000000?;4096654104697113=0806101273590052100000?

SS: Start sentinel (%)
FC: Format code
PAN: Primary account number
FS: Field separator (^)
CN: Cardholder's name (up to 26 characters long)
ED: Expiry date (in the form, "YYMM")
SC: Service code
DD: Discretionary date (may include the Card Verification Value [CVV]/Code, the PIN Verification Value, and the PIN Verification Key Indicator)
ES: End sentinel (?)
LRC: Longitudinal redundancy check

SS: Start sentinel (;)
PAN: Primary account number (up to 19 digits long)
FS: Field separator (=)
ED: Expiry date (in the form "YYMM")
SC: Service code
DD: Discretionary data
ES: End sentinel (?)
LRC: Longitudinal redundancy check

3 Steps to Multi Million Dollar Fraud

- Attack
- Sell
- Shop

The Underground Shopping Mall

- Malware Authors, Phishing Attackers, Skimmers, Exploiters Etc.
- Forums and Online Shops
- Buyers
- Specialized Services

Malware Authors, Phishing Attackers, Skimmers, Exploiters

- Financially Motivated.
- Insider threat, 3rd Party IT Service Provider, Outsider threat
- Background in Payment Processing and related service development

Forums and Online Shops

ANOTHER USA DUMPS UPDATE! / 25 SEPTEMBER 2014 / COMMENTS:

Guess what? USA Dumps update!

Base name: American Sanctions 14
Valid rate of: 92%
Track 1, Track 2, State/Zip.
Replacement time: 5 minutes

Buyers

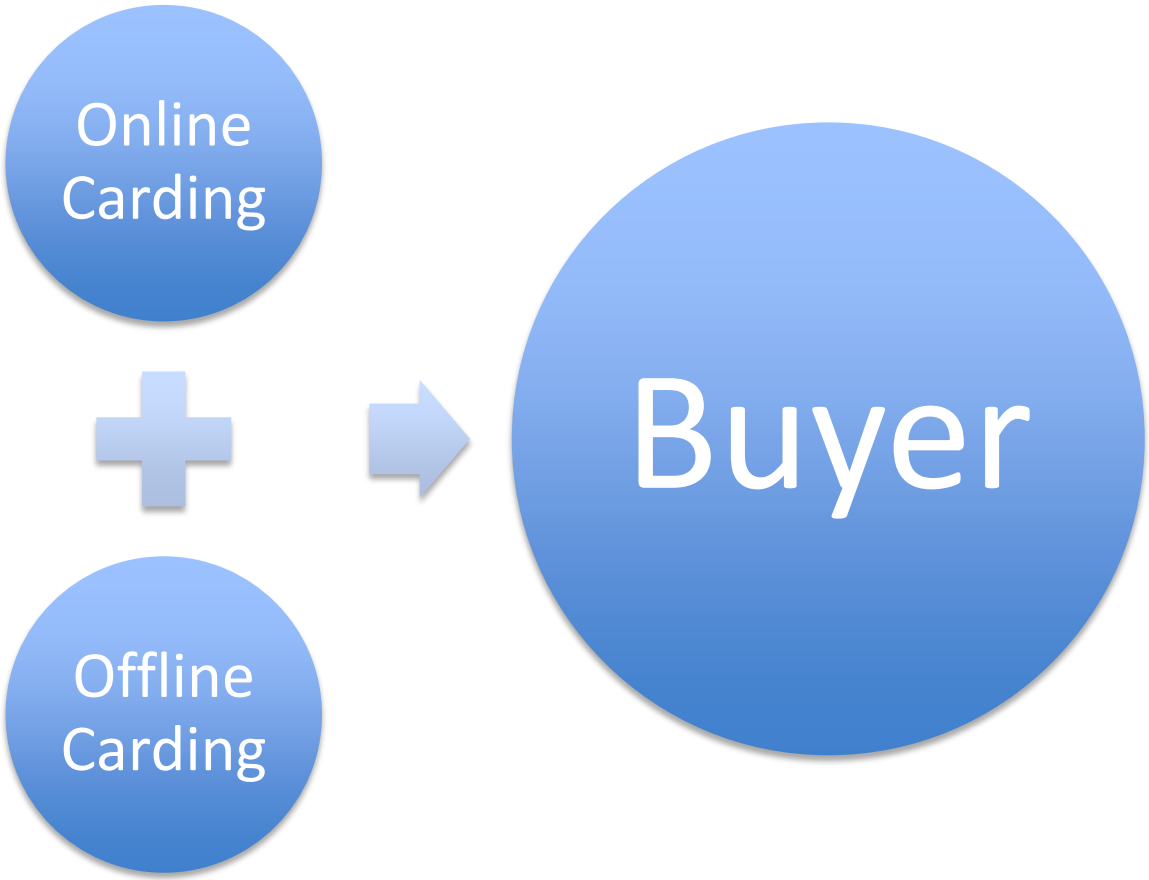
- Profile ranges from Newbies to Regular and experienced customers.
- Can Buy single CC, Dumps of Fullz.
- Can purchase cards with specific options like Country and City of issue, Card Issuer Bank, Brand(Visa, Master, Amex etc), Genre(Classic, Platinum, Gold etc)
- Purchase is made using Crypto currencies, wire transfer or money transfer.
- The price of a single card detail would depend on factors like Brand, Genre, expiry date etc.
- The cost of dump is calculated based on number of CC details it has.
- Fullz can be slightly more expensive than others as it contains more detailed information about the card owner.

Country	CC type	CC mark	Debit/Credit
All | USA	All | Visa | Master	All | Gold | Platinum	DEBIT CREDIT

Zips & Bins	Bank & State & City	Base	Additional
111 76282	Bank: All State: All City: All	All	Expiring 03/15 Phone VBV Exp. date (1312)

u were looking for? Need more dumps of particular bin? Try our partner's shop - Bulk Orders - Low Prices!

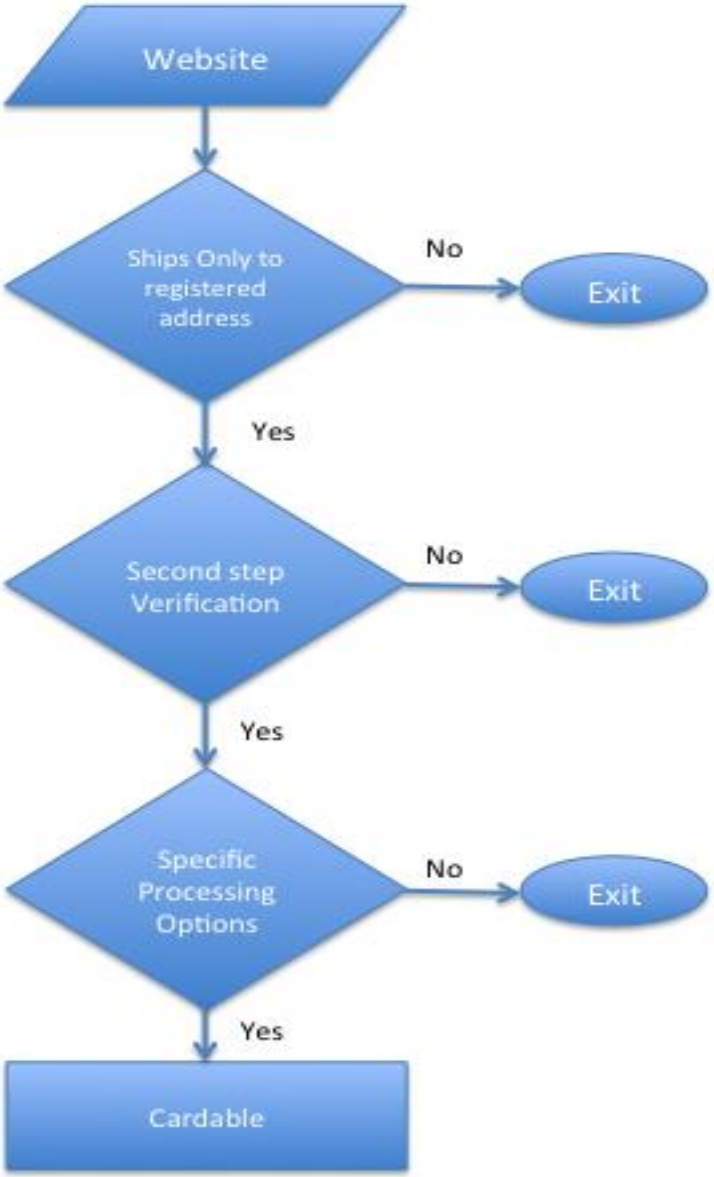
Clear Search


Online
Carding
Offline
Carding
Buyer

Online Carding

- Process of using the stolen credit card details for purchasing goods online.
- “Fullz” or details including CVV, Registered Address, Phone etc. is required.
- Finding a “Cardable” Website.

Cardable Website



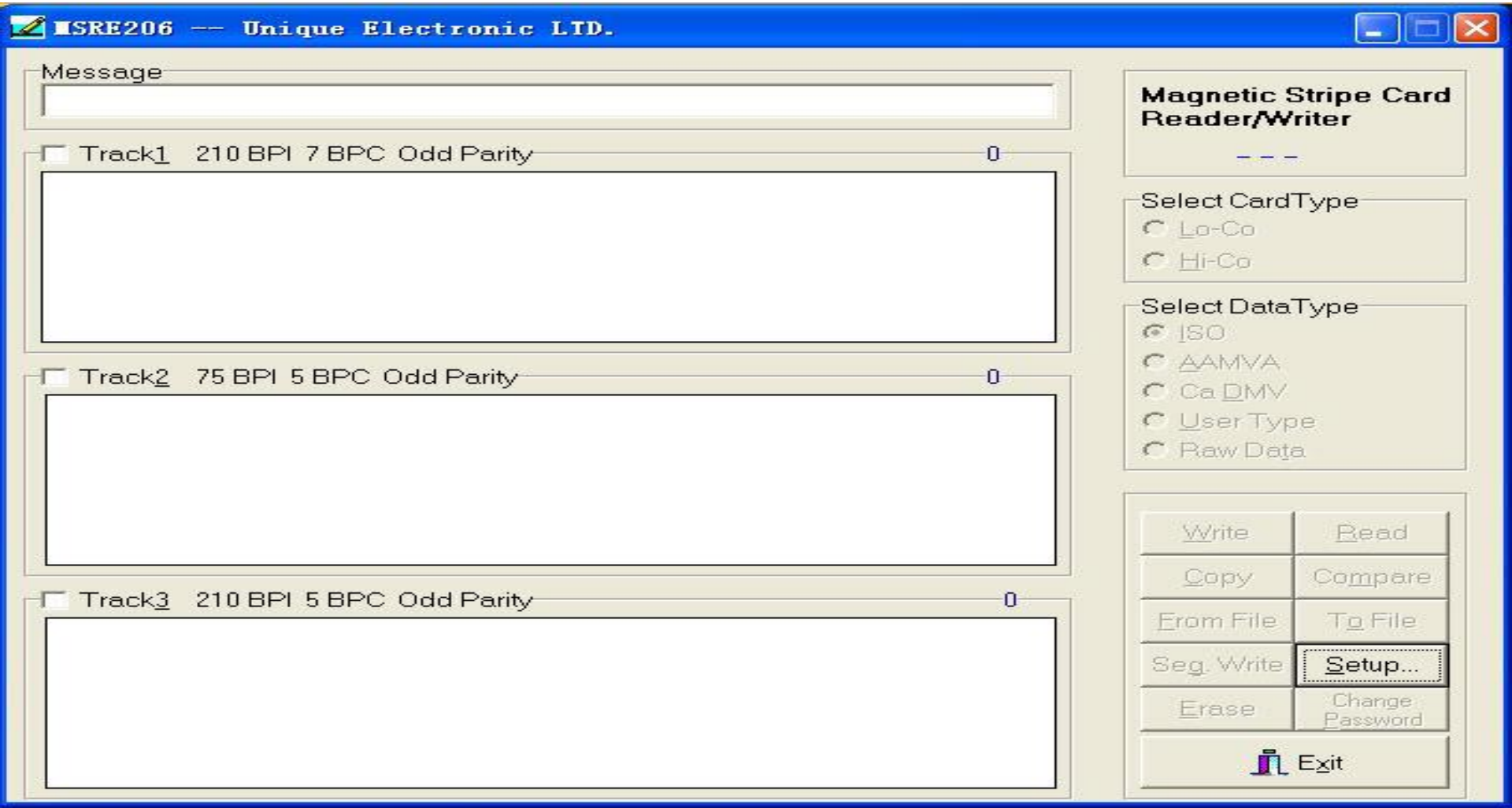
Offline/In-store Carding

- Generating Counterfeit cards.
- Choose shop/cash-out options.
- Pick up specialized services based on fraud options.

Generating Counterfeit Cards

Generating Counterfeit Cards

Software: MSRE, TheJerm, Exeba etc.



Specialized Services in Fraud Ecosystem

- Runner
- Dropper
- Shopper

Runners

- Individual or group specializing in ATM cash withdrawals.
- Often generate multiple counterfeit cards for single card to do multiple withdrawals In a go.
- Have Fake digital wallet, crypto currency, online money transfer accounts to safely withdraw money from 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.

vAn pErsie •

BS Trusted Seller

BlackStuff Top Level Seller

Join Date: Feb 2011

Posts: 1,366

Westernunion , Bank , Paypal , Moneybookers transfers !!!!!

{{ Western Union , Bank , Paypal & Money Bookers Transfers }}

Contact Me For Deal

Yahoo :van_persie619@yahoo.com
ICQ : 660941907

Hello BS members,

I'm a old and experienced carder,i have much data of westernunion,hacked paypal accounts,bank logins and fullz infos . I'm doing this business since last 8 years and also very old seller on blackstuff.net .I have many customers and buyers all over the world and they trust me and i promised to never break this chain till death . I'm offering here many offers to earn online money through black sources like westernunion transfers,bank transfers,moneybookers and paypal transfers through database.

Paypal Transfer Rates :

Code:

```
$1200 Transfer = $200 Charges (Payment Only BTC or PM)
$1800 Transfer = $250 Charges
$3000 Transfer = $300 Charges
$5000 Transfer = $500 Charges
$10,000 Transfer = $700 Charges
```

Bank Transfer Rates:

Code:

```
$1500 transfer = $250 Charges (Payment Only BTC or PM)
$2500 Transfer = $350 Charges
$5000 Transfer = $500 Charges
$10,000 Transfer = $1000
$15,000 Transfer = $1300
```

Western Union Transfer Rates :

Code:

```
$1400 Transfer = $250 Charges ( Payment only Via BTC or PM)
$2500 Transfer = $350
$3500 Transfer = $400
$5000 Transfer = $500
$7000 Transfer = $700
```

Terms & Conditions :

A person can take transfer once in a week and maximum 4 times in a month .
If anyone want to do regular business with me then you must have many bank accounts,paypal,moneybookers and fake ids for western union because after 2 or 3 transfers
your paypal and Wu ids will be black listed and banned. so think before deal. Make big transactions and get a side and give other peoples chance
or try to gather many fake accounts and work with me on regular basis.

Droppers

- Serves as the drop point for goods purchased online, thus securing the identity of the actual buyer
- Works by renting apartments, finding empty houses, registering PO Boxes on fake IDs.
- Since the Dropper bares a fair amount of risk, his profit percent varies between 30 to 50 percent.

CcWorld •

Verified Seller

Join Date: Jun 2013

Posts: 359

ccworld shipping provider world wide

Hello everyone ,

Today im here to inroduce my shipping services. i have lot of experience in carding business, starts from to card cheap softwares and online poker and casino games etc but when i joined big hacker communities and see big carders then i enhance my carding interest and starts working on carding ipads etc then i fuck amazon first time with 2 ipads and then i start to give 24/7 time to carding and net surfing and no]w i can card even big vehicles from ebay and amazon lol and also carding on walmart and bestbuy.

if you think this is a joke then you dont knows the real carders power.if you peoples trust me then i can show my carding skills.

I have some good drops in USA EU and many other countries.

Rules :

1: Order only with DHL, Fedex , TCS ,USPS, First flight, Canada post Available.

Fees and charges :

Normal Shipping :- (Shipment delivery direct from store to your house)

1: Laptops (Acer, Apple, Hp, Dell only) price starts from $350 to 500$

2: Iphones Apple (iphone5s for 250$)

3: Blackberry (Starts from 150$ to 300$)

4: Samsung Galaxy and Tabs (Starts from 150$ to 350$)

5: Apple Ipads or other tablets price $150

First Ship to drop, Last to customers (in this way i will ship item to my drop then he send it to you)

1: Laptops (Acer, Apple, Hp, Dell only) price starts from 300$ to 600$

2: Iphones Apple (iphone5s for 275$)

3: Blackberry (Starts from 200$ to 350$)

4: Samsung Galaxy and Tabs (Starts from 200$ to 400$)

5: Apple Ipads or other tablets price $200

Shipment Sites :-

Amazon
Ebay
Bestbuy
Walmart (special offers for USA customers only)

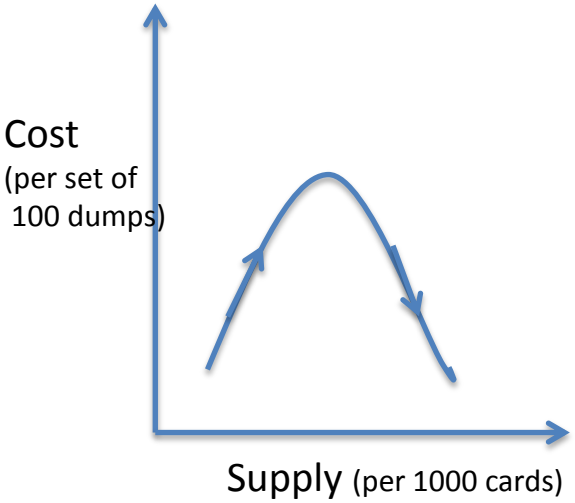
Shoppers

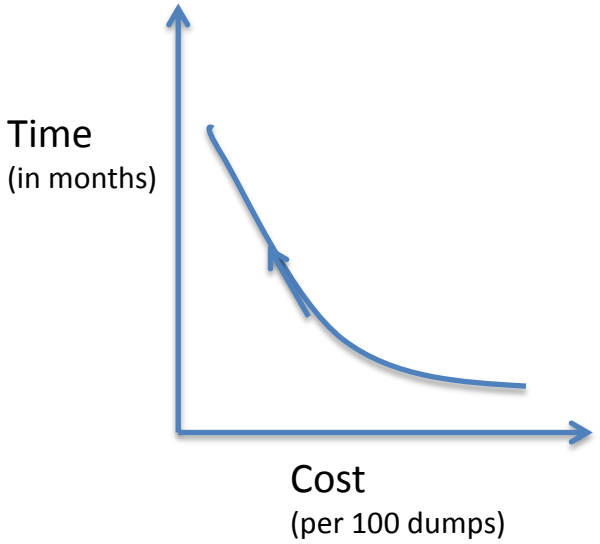
- Shopper specializes in shopping with the counterfeit cards provide by the carder.
- The Shopper can be an individual or a group that specializes in conducting nervousness-free shopping of goods using the fake cards.
- The shoppers also have Fail-safe techniques to doge the payment supervisor in case the card fails to authenticate.
- Profit cut in the range of 10 to 20 percent.
- 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.

Demand & Supply

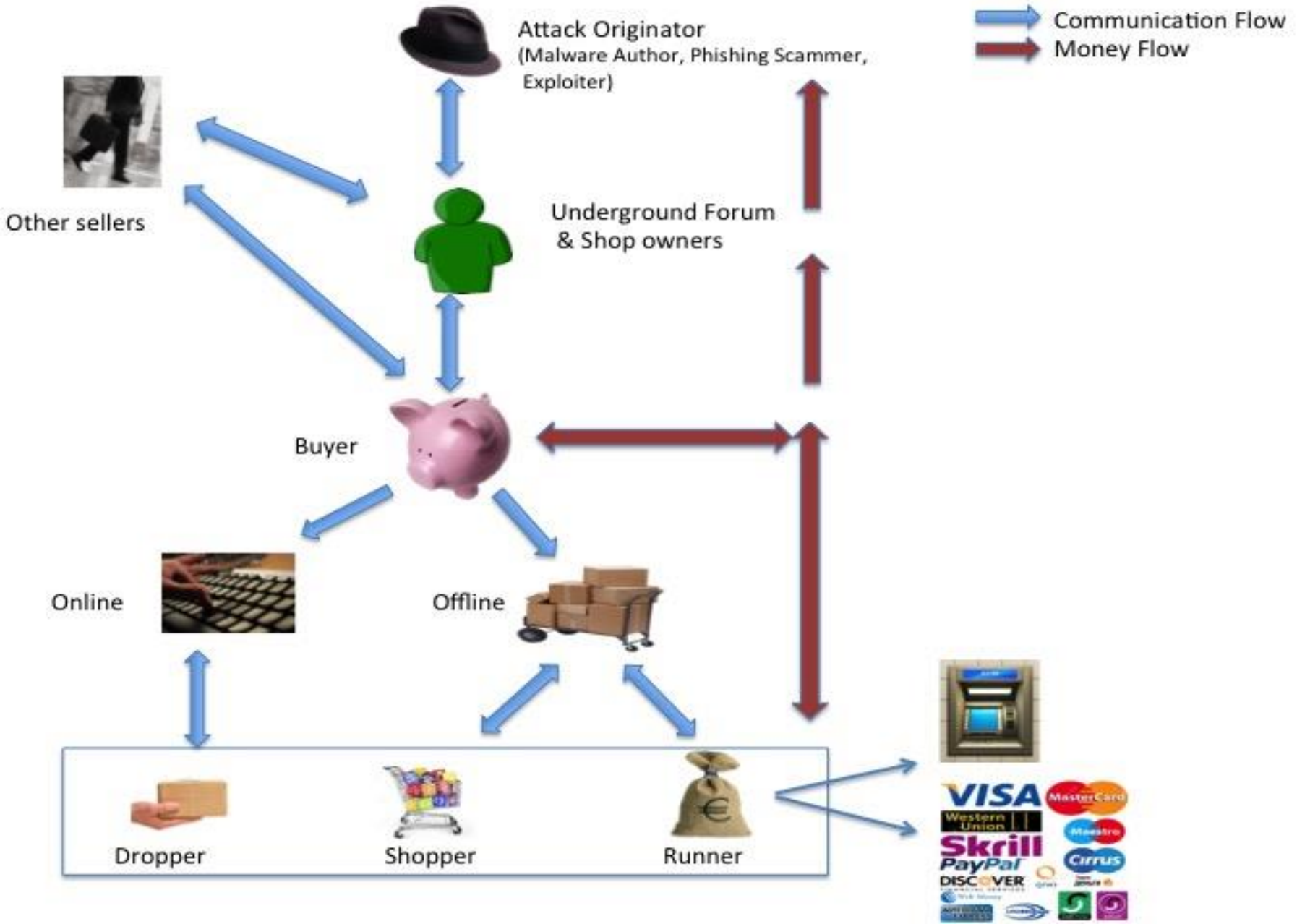
- Any new disclosure about POS breach suddenly raises the demand for fresh CC dumps in the market.
- This leads to a rise in price of new dumps.
- The problem arises when the demand is less and supply is huge.
- to keep up the momentum, the shop owners and sellers begin lowering the price of their dumps and cards. This brings down the market valuation thus creating deficit.

Demand & Supply





Credit Card fraud Ecosystem in a Nutshell



Future Scope, Challenges & Solutions

- Credit card fraud has been around for years now and with time, the model has grown stronger and better with each passing day.
- The major challenge that this ecosystem faces is double fraud.
- The payment industry has been dealing with this issue seriously but the problem lies in the widespread reach of card usage.
- Enforcing a global policy is not easy.
- Solutions like EMV or Chip-and-Pin cards and RFID cards exist.

Questions


SPEAKER
black hat
ASIA 2015
MARCH 24 - 27, 2015
MARINA BAY SANDS | SINGAPORE
WWW.BLACKHAT.COM