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

1. Cardholder purchases goods or services from the merchant

2. Merchant transmits the transaction to the Acquirer

3. Acquirer submits ticket to Issuer for payment

4. Issuer bills Cardholders

5. The Acquirer credits the Merchant for transactions

6. Aquirer is paid

7. Cardholder pays Issuer
Key Components
POS RAM Scrapping Malware In a Nutshell

RAM Temporarily Stores the Unencrypted Data

MAL.EXE Starts Reading the data in the Primary Memory

Running Processes

Meaningful Data is written on Disk

ERTFDFDGF!@$%^&TRYRTY^&HYT&^FGFDGFY^TGTQAQ#@%B4096654104697113^SINGH/ABHINAV^08061012735905210000000000000000?;4096654104697113=0806101273590521000000?#112$&&5yygfrbg*7567
Dumped Data

%B4096654104697113^SINGH/ABHINAV^
08061012735900521000000000000000?

;4096654104697113=080610127359005210000000?
Inside the Plastic Card

Track 1: Card number, holder name, expiration date.
Track 2: Card number, expiration date.
Track 3: Occasionally used by loyalty schemes.

Tracks:
1
2
3

Magnetic strip

Signature strip

Image source: Blog.cisco.com
Track 1 & 2 Block Diagram

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 data (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
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

Guess what? USA Dumps update!

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

Another USA Dumps Update! / 25 September 2014 / Comments:

POPEYES DUMPS

GOLDENDUMPS.CC

Dumps.cc - Online Dumps Shop| Checker Shop 24x7
iSwipe.CC Your new source of dumps, SWIPE IT GOOD!
 HUGE base, Quality dumps, Instant delivery
 LIVEFIRE.cc - COME PLAY WITH FIRE
 ***THE BIGGEST EU DUMPS BASES*** ICQ: 675281103

OVER 2.5 MILLION DUMPS ONLINE
FRESH DUMPS FOR SERIOUS CUSTOMERS ONLY
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.
<table>
<thead>
<tr>
<th>Country</th>
<th>CC type</th>
<th>CC mark</th>
<th>Debit/Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>All USA</td>
<td>All</td>
<td>All</td>
<td>DEBIT CREDIT</td>
</tr>
<tr>
<td>Zips &amp;Bins</td>
<td>Bank &amp; State &amp; City</td>
<td>Base</td>
<td>Additional</td>
</tr>
<tr>
<td>111</td>
<td>Bank: All</td>
<td>All</td>
<td>Expiring 03/15</td>
</tr>
<tr>
<td></td>
<td>State: All</td>
<td></td>
<td>Phone</td>
</tr>
<tr>
<td></td>
<td>City: All</td>
<td></td>
<td>VBV</td>
</tr>
<tr>
<td>76282</td>
<td></td>
<td></td>
<td>Exp. date (1312)</td>
</tr>
</tbody>
</table>

You were looking for? Need more dumps of particular bin? Try our partner’s shop - [Bulk Orders - Low Prices](#)!
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

Website

Ships Only to registered address
- No: Exit
- Yes: Second step Verification

Second step Verification
- No: Exit
- Yes: Specific Processing Options

Specific Processing Options
- No: Exit
- Yes: Cardable
 Offline/In-store Carding

• Generating Counterfeit cards.

• Choose shop/cash-out options.

• Pick up specialized services based on fraud options.
Generating Counterfeit Cards

- Magnetic Stripe Reader
- Plastic cards/Expired cards/Counterfeit printed cards
- Encoder Software
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.
Westernunion, Bank, Paypal, Moneybookers transfers !!!!!

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

Contact Me For Deal

Yahoo: van_persle619@yahoo.com
ICQ: 660941907

Hello BS members,

I'm an 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.
Hello everyone,

Today I'm here to introduce my shipping services. I have a 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 start 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 now I can card even big vehicles from eBay and Amazon lol and also carding on Walmart and Best Buy.

If you think this is a joke then you don't know 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

- Cost (per set of 100 dumps)
- Supply (per 1000 cards)

- Time (in months)
- Cost (per 100 dumps)
Credit Card fraud Ecosystem in a Nutshell

- **Attack Originator** (Malware Author, Phishing Scammer, Exploiter)
- **Underground Forum & Shop owners**
- **Buyer**
- **Other sellers**
- **Communication Flow**
- **Money Flow**

**Online**
- **Dropper**
- **Shopper**
- **Runner**

**Offline**
- **VISA**
- **MasterCard**
- **Skrill**
- **PayPal**
- **Discover**

**Cards**
- **Visa**
- **MasterCard**
- **Skrill**
- **PayPal**
- **Discover**
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