Bullet-Proof Credit Card Payment Processing

Damon McCoy
New York University

Joint work with Stephen M. Gaffigan, P.A. and Sean West
Mapping out Dependencies

Figure credit: Christian Kreibich
Merchant Banks (Late 2010)

- Low diversity
  - 3 banks cover 95% of spam
  - Fewer banks willing to handle “high-risk” merchants
- High switching cost
  - In-person account creation, due diligence, multiple days…
  - Upfront capital, holdback forfeiture

Levchenko, Pitsillidis, Chachra, Enright, Felegyhazi, Grier, Halvorson, Kanich, Kreibich, Liu, McCoy, Weaver, Paxson, Voelker and Savage, *Click Trajectories: End-to-End Analysis of the Spam Value Chain*, Oakland 2011
“Right now most affiliate programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program imho, there is a general sad picture, fucking Visa is burning us with napalm (for problematic countries, it's totally fucked, on a couple of programs you're lucky if you get 50% through).”
Luxury Goods
Payment Intervention

• STEPHEN M. GAFFIGAN, P.A. and Sean West

• Started on July 9th 2014 with 4 brand holders
Payment Processors

- Middlemen between merchants and acquirers

Issuing Bank

Acquiring Bank

VISA

MasterCard

First Data

Joe's PIZZA
Aside: Trace Purchasing

- Can’t provide a URL to Visa/MasterCard
  - They have no mapping between merchant account and URL

- Identifying merchant account requires a trace purchase
Compromised Websites

cheap beats by dre site:edu

About 37,400 results (0.38 seconds)

cheap dr dre beats solo headphones - Talladega College
www.talladega.edu/?newbeats-51.html  Talladega College  ·  etc
beats by dre warranty email Black Friday · cheap beats by dre solo in blue Black Friday · monster beats by dr. dre studio preisvergleich · monster beats by dre ...

create beat cheap monster cheap beats dr dre dre html ...
www.talladega.edu/?newbeats-3374.html  Talladega College  ·  etc
where can i get cheap monster beats Black Friday · dr dre beats at best buy Black Friday · how long is the warranty on cheap beats by dre Black Friday ...

cheap beats by dre studio cheap - Talladega College
www.talladega.edu/studentlife/sl.asp?newbeats-11991...  Talladega College  ·  etc
cheap beats by dre studio cheap monster beats by dr. dre studio high-definition headphones intra beats by dre. beats by dre studio battery life Black Friday | dr ...

wholesale beats by dre tour Beats by Dre Cheap China
cdl.ucla.edu/?q=news/ZDEzNTk0  ·  Cuneiform Digital Library Initiative  ·  etc
wholesale beats by dre tour. Wholesale 10pcs monster beats by dr.Dre tour in ear headphone wholesale beats by dre tour for sale. About offer sign in register.
Counterfeit Sites
Payment Gateways

SECURE PAYMENT

Payment To: www.perfectshoessmarket.com

Details of your order

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Product No.</th>
<th>Quantity</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>168.9 USD</td>
</tr>
</tbody>
</table>

Shipping: 30 USD Payment Amount: 198.90 USD

Information of Bills

Credit Card Information

Card Type: 
Card Number: *
Expiration Date: 07 4 2017
CVV2: *

Billing Address:
Post Code:
Billing City:
Email:

*Notes:
You are now connected to a secure payment site with certificate issued by VeriSign.
Your payment details will be securely transmitted to the Bank for transaction authorization in full accordance with PCI standards.
Bullet-Proof Credit Card Payment Processors
Standard Fraud Detection
Bypassing Fraud Detection
Test Purchase Blocking

- Blacklisting IP addresses, Credit Cards, Billing addresses, and names
  - Easy to change except for name

- Tracking and fingerprinting devices

- Blocking repeat purchasers for certain brands

- Sharing customer information between processors
Larger Network
Test Purchasing Results

• 17 Months

• 3 banks underwrite 97% of accounts

• 15 Payment facilitators

• 313 successful test purchases

• 242 unique merchant accounts
  ➤ All terminated or in the process of being investigated
BP Processing Model

- 5,000 RMB (~$775 USD) annual fee
- 4-6% transaction fees
- Fines are not passed to merchants
- T + 20 holdback
Banks

• 97% of accounts underwritten by three banks
Summary

• BP processors aiding spammers by blocking test purchases

• Banks continue to work with BP processors

• Unknown Visa enforcement on repeat offender banks
RealyPay Closed Down