Economics and the Underground Economy

Cormac Herley and Dinei Florêncio
Microsoft Research, Redmond
Everybody Knows Cybercrime is Big Money
“Everybody knows Phishers make lots of money ….”

- AntiPhish WG graphs
  - Growth in # sites
- Gartner Surveys:
  - 2005 “$929 mln”
  - 2006 “$2.1bn”
  - 2007 “$3.2 bn”
Everybody Knows:
Cybercrime (e.g. IRC) Markets are Big Money

How do we know this?

- **Black Market In Credit Cards Thrives on Web**

- **The Underground Economy: priceless**
  - “Even those without great skills can barter their way into large quantities of money they would never earn in the physical world.”

- **Symantec Underground Economy Survey**
  - “Symantec has calculated that the potential worth of all credit cards advertised during the reporting period was US$5.3 billion.”

- **A Field Day for Financial Cyber-Scammers**
  - “Total losses from cyber-related crime at financial institutions topped $20 billion last year, estimates security consultant Lance James”
Generates work for Graphic Designers
A Few Things That Make No Sense
Why do Credentials sell for pennies on dollar?

- Symantec: “CCN’s sell for $0.5 to $12”
- Cymru: $500 for face value $10million creds
- Franklin etal.: 465 free CCNs/day on single channel

Offered Explanations:
- More supply drives price down [Symantec]:
  - But demand for free money is infinite?
- Volume Sellers don’t care [Cymru]:
- Nobody sells gold for the price of silver
How Can Market Function when Cheating is Common?

- **Thomas & Martin:**
  - “Each IRC network will normally have a channel, such as #help or #rippers, dedicated to the reporting of those who are known to conduct fraudulent deals.”

- **Symantec:**
  - Many IRC servers have channels listing current rippers

- **Franklin et al:**
  - 22% of posted CCNs failed Luhn checksum
  - Utilities provided by channel admin designed to steal CCNs

- **Dhanjani and Rios [Blackhat08]:**
  - Backdoors common in for-sale phishing kits/tutorials

- **Cova et al:**
  - Obfuscated backdoored phishing kits

**Countermeasures ought to be easy**
Why is cheating common?

- Why does anyone bother putting backdoors in phishkits if easy money lies all around?
- Why steal $0.50 / CCN if you can do the real stuff?
Where are the bodies?

- Phish victims 2008: 5 million
  - [Gartner]

- US job losses July 08-June 09: 5.3 million
  - [Dept. of Labor]

  - Online and paper journalists
Where’s the loot?

- Gartner estimates: “$3.2 bn lost to phishing in 2007”
  - > TacoBell revenue $1.8bn
- FTC 2005 estimate: $47bn in ID theft
  - > earnings of top 5 US banks 2005
  - > $100k each for 0.5 million ID thieves
- When things are big they’re visible
  - Even if they try to hide
Banks do little

- Negligible 2-factor deployment in US
- Cosmetic measures: e.g. SiteKey
- US banks entirely silent on losses
  - No published numbers
  - No demands for legislation (Remember DMCA?)
- Don’t seem worried:
  - “We guarantee that you will be covered for 100% of funds removed from your Wells Fargo accounts in the unlikely event that someone you haven't authorized removes those funds through our Online Services.”
  - “We will reimburse your Fidelity account for any losses due to unauthorized activity.”
Users do less

- Choose weakest passwords
- Anti-Virus installed? Current? Running?
- Ignore certificates
- Click on anything.
- Uptake on phishing protection low.
- Automatic updates?
Laws of Economics have not been suspended

- Competition decreases return
  - When it’s raining money, there are always enough people with buckets
- Tragedy of the Commons
  - If anybody can do it, everybody does
- Market for Lemons
  - Cheating on IRC channels makes commerce impossible
- Firms are better than freelancers
  - Two Tier system
- W/o barrier to entry returns are bad
Phishing as Tragedy of the Commons

“And Simon answered, Master, we have fished all night, and caught nothing.”

Luke 5:5
Looks like the perfect scam

- Harvest free money
- Be 1000 miles from scene of crime
- Get everything you need online
- No capitol outlay, no training
  - Anybody can do it!!!!
- Except,
  - If anybody can do it, everybody does it
  - If everybody does it, nobody makes any money
Fishing and Phishing

- Both have predator-prey dynamics
  - Prey: fish or dollars
  - Predator: fishermen or phishers
- Fishermen are never rich
- Open access to the resource, i.e. no barrier
  - Anyone who wants to fish/phish can exploit
- Tragedy of the Commons
  - Fishing ground yields far less than it is capable of
  - Phishing yields far fewer dollars than possible
A Quick lesson in Competition

Return = \frac{\text{Victims}}{\text{Phishers}}

More Phishers

Less Phish?
The squeeze on phishing

- Return = Victims/Phishers
- Denominator increasing ("free money!!!!")
- Numerator decreasing
  - Technical measures: browser warnings etc
  - Fraud detection: banks get better
  - Users learn: nobody gets phishing 10 times.
Conclusions

- **Activity ≠ Dollars**
  - Amount of phishing email/sites indicates denominator is increasing
  - Things are getting worse for phishers, not better

- **The easier phishing gets the lower** $R_{\text{tot}}(E)$

- **Phishing is a low-skill low-rewards business**
  - Avg phisher makes ~ lost opportunity costs

- **Return = Victims/Phishers**
  - Denominator increasing, numerator decreasing
What about all the estimates showing that Phishing is HUGE??

  - Selection Bias: how contact unbiased sample email users?
  - Refusal Rate: those who respond to Gartner spam more/less likely to respond to phishing spam?
  - Telescoping: users throw-in incidents outside interval
Surveys: Exaggeration of Losses

- Very Small number of victim respondents
  - E.g. Javelin (Gartner) 2005 found 3 (25) victims resp.
- Dollar numbers are averages over victims
- **Victims who exaggerate hugely influence avg.**
- Speculation?
Our Estimate:
US phish victims: 0.4% of users per year

- **Gartner**
  - Users who say they were phished: 3.2%
  - Survey 4000
- **Clayton&Moore**
  - User credentials at hacked phish site: 0.34%
  - Hacked phishing site
- **Florêncio&Herley**
  - Toolbar users entering pwds at phish sites: 0.4%
  - Toolbar data, 500k users
Where are the bodies?

- Gartner “5 million lost money in 2008”
- Number of people in US who lost money
  - > # babies born in the US (3.9 million)
  - > # deaths in the US (2.4 million)
  - > # HS grads (2.9 m)
  - > # Suckers (assuming one born every minute: 525k = 365×24×60)
Our Estimate: Victims x Loss
US annual phishing losses = $60 million

- Assume Gartner median loss: $200
- Assume 50% of fraud successful
  - $200 \times 175e6 \times 0.037 \times 0.5 = $60 million
APACS (UK payments assoc):
- 2007 Online fraud = 22.6 GBP ~ $31.5 mln
- Assume 50% of online fraud is phishing
- Scale from UK pop to US:
  \[ \frac{31.5 \times 0.5 \times 300}{60} = 78.5 \text{ mln} \]
- Paypal CSO: “phishing is not even in the top five fraud loss threats Paypal faces”
  \[ \text{[darkreading 2007]}. \]
Do banks fear phishers or customers?

- Bank CEO is more afraid of:
  - Phishers
  - Own Customers

- Phishing loss: $60/175 = $0.34 per user/year
  - i.e. Avg. loss/customer < First Class Stamp
- Agent assisted phone call: $10/call
- 10% of customers making one call dwarves phishing all losses.
- “And you want me to roll out 2-factor to these people??”
Users are not irrational

- Banks cover the *direct* losses
- Regulation E limits user liability to $50
  - *even when the customer is negligent*
- Users are not irrational
  - Strong passwords, parsing URLs, understanding certificates is effort to save someone else money.
- Real cost for users is effort/hassle/headache
- If phishers steals $50, it’ll take a lot more than $50 in time/effort to explain/figure out.
Spam is more expensive than AdWords/AdCenter

“spam may be free, but it’s not cheap”
SPAM vs. ADS: which one is cheaper?

Competitive equilibrium: if enough advertisers can choose between the two, they should reach similar pricing (ROI).
SPAM vs. ADS: which one is cheaper?

Competitive equilibrium: if advertisers cannot choose, prices could be different. But there are some constraints.
SPAM vs. ADS: which one is cheaper?

Competitive equilibrium: if enough advertisers can choose between the two, they should reach similar pricing.

“SPAM is cheaper” would require:
- No business currently in AdWords/AdCenter could use spam instead
- (are there enough legitimate ads outside the reach of US spam laws?)

“SPAM is more expensive” would require:
- No business currently in SPAM could use AdWords/AdCenter.
- (are there any legitimate ads using SPAM?)

SPAM is more expensive then legitimate ads or campaigns!
SPAM: Are spammers making any money?

Supply-and-demand equilibrium:
- Buyers willing price&quantity = Sellers willing price&quantity
SPAM: Are spammers making any money?

Supply-and-demand equilibrium:
  - Buyers willing price&quantity = Sellers willing price&quantity
  - Marginal Demand: At this price, no buyers are willing to buy more services
    - => “total” cost is not cheaper than alternatives.
  - Marginal Offer: At this price, no (current or prospective) sellers are willing to provide more merchandise
    - => profit is slim, Sellers cannot be making much money. (no barrier to entry markets)

Spammers are not making much money.
SPAM

Spam is cheap BUSTED
SPAM

Spamming is easy money BUSTED
Underground Markets

“the underground economy has reached a very specialized division of labor”
Paradox 1: Creds sell for pennies on dollar

- Symantec: “CCN’s sell for $0.5 to $12”
- Cymru: $500 for face value $10 million creds
- Franklin et al.: 465 free CCNs/day on single channel

- Offered Explanations:
  - More supply drives price down [Symantec]:
    - But demand for free money is infinite?
  - Volume Sellers don’t care [Cymru]:
Paradox 2: How Can Market Function when Cheating is Common?

- **Thomas & Martin:**
  - “Each IRC network will normally have a channel, such as #help or #rippers, dedicated to the reporting of those who are known to conduct fraudulent deals.”

- **Symantec:**
  - Many IRC servers have channels listing current rippers

- **Franklin et al:**
  - 22% of posted CCNs failed Luhn checksum
  - Utilities provided by channel admin designed to steal CCNs

- **Dhanjani and Rios:**
  - Backdoors common in for-sale phishing kits/tutorials

- **Cova et al:**
  - Obfuscated backdoored phishing kits
These Paradoxes help explain each other:
Market for Lemons

Akerlof ‘70

- Seller knows quality better than buyer
  - Cars: is this a lemon or not?
  - CCNs/creds: am I a ripper or not?
- Buyers will pay only the average
What Causes a Lemon Market?

1. Asymmetry of Information
   ✓ Are you a ripper or not?
2. No credible disclosure
   ✓ Rippers are indistinguishable from real sellers
3. Low seller quality
   ✓ Rippers abound
4. Lack of regulation/assurance
   ✓ Anonymous irreversible transactions

IRC channels classic example of Lemon Market
The Ripper Tax

- Fraction $q$ of transactions are with rippers
- Can we estimate tax rate $q$?
  - Recall none of [Cymru, Symantec, Franklin, .......] has observed a single transaction
- But Tragedy of Commons argues that it is high
  - IRC channel is Open Access resource pool for rippers
  - =>Resource overgrazed
- Three main factors reduce price of CCN
  - Banks detect fraud e.g. 90%
  - Buyers demand premium e.g. 5x
  - Rippers offer worthless CCNs e.g. 90%
  - $2000 \times 0.1 \times 0.2 \times 0.1 = 4$
Avoiding the Ripper Tax: Formation of Gangs and Alliances

- Coase: “Nature of the Firm”:
  - When transactions are taxed or uncertain it makes sense to form groups rather than buy/sell in a market.
  - After a transaction with non-ripper makes more sense to deal with them again rather than pool of rippers/non-rippers
Two Tier Underground Economy

- **Tier 1:**
  - Avoid ripper tax
  - Extract all value from goods

- **Tier 2:**
  - Extract only part of value
  - No choice but to pay ripper tax

- Relying on markets for up/downstream services
  - Pay ripper tax on every transaction
Why do these markets exist?

- Activity is real: e.g. 100k users/server

Why does anyone trade in Lemon Market?

- New entrants/need relationships
- Sell resources that have no value to them
  - Cannot monetize
  - Sell kits/services with zero marginal cost
- Intend to cheat others
Effort => Desperation

- Nobody sells in a Lemon Market if they have a choice
- Activity => there are a lot of people with no choice
- Goods are easy to acquire, hard to monetize
  - Creds, CCNs, SSNs etc
Symantec:
“Potential value of CCNs stolen $5.3bn”

- Total CCNs offered for sale: 46k CCNs
- Sum of asking prices: $163 million
- [Total offered for sale] x FTC Avg CCN fraud = $5.3 billion
- So Symantec estimate = [Sum of asking prices] x 32
- This assumes:
  - 100% of goods offered on IRC channels sell (at asking price)
  - Banks detect 0% of attempted fraud
  - Rippers account for 0% of sales
  - Sellers give buyers 30x return
Buyers demand 5x return
Final price 50% of ask
Assume 10% of offered creds sell *and* are good

Total CC fraud from channels:
\[ 163 \times 5 \times .5 \div 10 = $41 \text{ million} \]

Factor difference with Symantec: 128x
  - Extrapolating from $0 to $5.3 bn is a big jump
“But, they wouldn’t be doing this if they weren’t making money”
**Effort ≠ Dollars**

Phishing
- Denominator increasing
- Numerator decreasing

Spam

IRC channels:
- Newbies
- Rippers

Prospectors on the way to the Klondike 1897
Cannot estimate the gold in the mountains by activity at the shovel store

- News of Klondike gold strike July 1897
- Attempt to reach: 100000
- Reach Klondike: 20000
- Find any gold: 4000
- Get rich (> $5k): 300

- Gold extracted: $50 million
- Goods sold to prospectors: $100 million
“They wouldn’t be doing it if they weren’t making money”

- No. They think they’re going to make money
- Where would they get that idea?

- **Black Market In Credit Cards Thrives on Web**
  - "Want drive fast cars?" asks an advertisement, in broken English, atop the Web site iaaca.com.
  - "Want live in premium hotels? Want own beautiful girls? It's possible with dumps from Zoomer."

- **The Underground Economy: priceless**
  - “Even those without great skills can barter their way into large quantities of money they would never earn in the physical world.”

- **Symantec Underground Economy Survey**
  - “Symantec has calculated that the potential worth of all credit cards advertised during the reporting period was US$5.3 billion.”

- **A Field Day for Financial Cyber-Scammers**
  - “Total losses from cyber-related crime at financial institutions topped $20 billion last year, estimates security consultant Lance James”

When we encourage overestimation of returns we make things worse.
Ironies

- Irony: Whitehats recruit their own opponents
  - Dubious reports of cybercrime riches
  - Recruits new entrants to Tier 2
  - Contribute to spam/phishing
- Irony II: realistic estimates benefits (almost) all
  - Who benefits: Banks, Users, InfoSec comm, Tier 1, Tier 2
  - Who suffers: Rippers
A few things that start to make sense
Credentials and Rippers

- Rippers abound on IRC channels
  - Cheating works because of newbies
- Creds sell for pennies on the dollar?
  - Most on IRC channels are junk
  - Creds easy to acquire, hard to monetize
Where are the bodies/loot

- Why so hard to find 5 million phishing victims
  - Off by 10x
- Who lost $3.2 billion
  - Off by 50x
Banks and Users

- Banks and Two-factor
  - Average loss/user/year $0.34

- Users have no liability for direct losses
  - Ignoring security advice rational
So you’re saying Cybercrime is no big deal?
Kanich et al. [Pharma campaign]
- 350 million emails
- 28 sales
- $2731
- Indirect costs > 10 x direct costs
  - 1% got into inboxes, 2 seconds/recipient, 2xmin wage: $28k
  - Also, bandwidth, storage, provisioning
## Direct and Indirect Costs

- **Direct costs**: zero-sum game
- **Indirect costs**: negative sum

<table>
<thead>
<tr>
<th></th>
<th>Direct Costs</th>
<th>Indirect Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishers</td>
<td>$+60 million</td>
<td>Don’t care</td>
</tr>
<tr>
<td>Banks</td>
<td>$-60 million</td>
<td>Customer support, new technology, Reputation, fraud detection.</td>
</tr>
<tr>
<td>Users</td>
<td>$0</td>
<td>Time, Effort, hassle</td>
</tr>
</tbody>
</table>

- **Indirect costs >> direct costs**
Direct Losses and Externalities

- Tier 1 probably gets the bulk of the direct gains.
- Externalities are caused by all who spam/phish (not just those who do it well).

Harder to apply economic incentives to Tier 2
Conclusions
Conclusions:

- Stuff on IRC channels
  - Easy to acquire, hard to monetize
- Effort $\neq$ dollars
  - Amount of spam, phishing etc not indicative of profit
- Cybercrime is a ruthlessly competitive predatory industry
  - Low-skill dead-end jobs
- Published cybercrime estimates hugely exaggerated
- Repeating claims makes matters worse.
Conclusions: Underground markets

- “Underground Markets are easy money”
  - Violates basic economics
  - Defies common sense
  - Contradicts experience from other crime
  - Unsupported by evidence
- Stories about “easy money” in cybercrime are so 2006
REFERENCES