Buying Drugs for Science: Addressing the Economics of Cybercrime

Stefan Savage
UC San Diego

joint work w/Neha Chachra, Brandon Enright, Mark Felegyhazi (ICSI), Chris Grier (Berkeley), Tristan Halvorson, Chris Kanich, Christian Kreibich (ICSI), Kirill Levchenko, He “Lonnie” Liu, Justin Ma, Damon McCoy, Vern Paxson (ICSI/Berkeley), Andreas Pitsillidis, Geoff Voelker, and Nick Weaver (ICSI)
Computer security is a technical problem
- There are some software or design flaws
- These flaws can be exploited by adversaries

If we fix these technical problems then we will be secure

But you better get them all because the adversary is adaptive...
But, today’s best practices...
... have not stopped our adversaries
Profit driven e-crime

- The largest driver for threats is $$$
  Scale allows commodity monetization
  Engenders complex value chain relationships
Today: the spam ecosystem
Affiliate program structure

- Division of labor
  - **Affiliates** handle advertising (e.g., spam, SEO)
    - Independent contractors
    - Paid 25-60% commission depending on kind of program
  - **Affiliate programs** handle backend
    - Payment processing, customer service, fulfillment
    - Sometimes hosting and domain registration

- Why?
  - Transfer of risk: innovation risk vs investment risk
  - Specialization lowers cost structure
10% of affiliates account for ~80% of total program revenue.
Direct costs: 70.8%
Indirect costs: 12.8%
Profit: 16.3%

<table>
<thead>
<tr>
<th></th>
<th>RX-Promotion March – September 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gross revenue</strong></td>
<td>$7.8M</td>
</tr>
<tr>
<td><strong>Direct costs</strong></td>
<td></td>
</tr>
<tr>
<td>Commissions</td>
<td>$3M (38.1%)</td>
</tr>
<tr>
<td>Suppliers(^a)</td>
<td>$1.4M (17.6%)</td>
</tr>
<tr>
<td>Processing</td>
<td>$1M (13.2%)</td>
</tr>
<tr>
<td>Other direct</td>
<td>$148.3K (1.9%)</td>
</tr>
<tr>
<td><strong>Indirect costs</strong></td>
<td>$1004K (12.8%)</td>
</tr>
<tr>
<td>Administrative</td>
<td>$197K (2.5%)</td>
</tr>
<tr>
<td>Customer service</td>
<td>$124K (1.6%)</td>
</tr>
<tr>
<td>Fines</td>
<td>$107K (1.4%)</td>
</tr>
<tr>
<td>IT expenses</td>
<td>$202K (2.6%)</td>
</tr>
<tr>
<td>Domains</td>
<td>$114K (1.5%)</td>
</tr>
<tr>
<td>Servers, hosting</td>
<td>$66K (0.8%)</td>
</tr>
<tr>
<td>Selling expenses</td>
<td>$315K (4%)</td>
</tr>
<tr>
<td>Marketing</td>
<td>$105K (1.3%)</td>
</tr>
<tr>
<td>Lobbying</td>
<td>$157K (2%)</td>
</tr>
<tr>
<td>Other indirect</td>
<td>$134K (1.7%)</td>
</tr>
<tr>
<td><strong>Net revenue</strong></td>
<td>$1.3M (16.3%)</td>
</tr>
</tbody>
</table>
Click Trajectories

- Click Trajectory project
  - Find “bottlenecks” in the spam value chain
  - Place where intervention could be most effective
    - Resources with largest impact on profitability
    - Highest switching cost for adversary

- Measure empirically
  - Resources needed to monetize each piece of spam
  - By playing the role of customer; at scale
    - Three domains: pharma, replica, software
Click Trajectories study [Levchenko, IEEE S&P 2011]

Aug 1 -- Oct 31 2010

7 URL/Spam feeds + 5 botnet feeds
- 968M URLs, 17M domains
- 99% of pharma, OEM, replica

Crawled domains for 98% of URLs in
- 1000s of Firefox instances
- Large IP address diversity

Hundreds of purchases
- Unique card # per order
- Full transaction data
Example: What if you ordered from these guys?

Bank Identification Number (BIN) 448314

Merchant descriptor “Smart rt online”

Card Acceptor ID “8875236”

Merchant Category Code (MCC) 5912
Drug Stores & Pharmacies
600+ orders later...
The big finding

- Most resources are cheap and plentiful
- Replacement cost < expected profit
  - This is why shutting down domains and Web sites is unlikely to ever work
- One major exception...
Merchant banks (circa late ‘10)

- Low diversity
- 3 banks covered 95% of pharma/replica/software spam
- Fewer banks willing handle “high-risk” merchants
- High switching cost
- Time: In-person account creation, due diligence
- Money: Upfront capital, holdback forfeiture (big deal)

Hypothesis: Targeting merchant accounts could have major impact

- St. Kitts & Nevis
- AGBank
- DnB NORD
Anecdotal evidence: Revenue by drug type (RX-Promo)
Nice academic result, but so what?

- A stew of activities
  - Encouragement from D.C.
  - Brand interest
  - Card association cooperation
  - Complex politics around SOPA/PIPA/etc
- Two major changes
  - Visa Global Brand Protection Program (GBPP)
  - Targeted merchant intervention (IACC & brands)
Targeted payment intervention today

- **Undercover** test purchase at counterfeit site
  - Get merchant bank BIN from transaction
  - IP holder notifies card network (e.g., Visa/MC)
    - Investigation; complaint delivered to merchant bank
- **Leverage via card association contract**
  - Merchant bank owns liability
  - Fines, increased scrutiny, de-association
- Merchant account shutdown
So... does it work?

- Bottom line: Yes, amazingly well.

- We’ve tracked bank association w/affiliate programs for almost two years (continuing...)
  - ~1000 purchases (Visa only)
- Joined programs as affiliates to get damage assessment from inside

- Quick stories: OEM software and Pharma
Major OEM affiliates
Microsoft’s Thanksgiving present (Nov ‘11)
- Methodically issued complaints for accounts of every major affiliate program
- Diligent follow-up: new processing > new complaints (and quickly)

Refusals increase as takedowns start

Scramble to find stable new bank
11/2011: Microsoft starts merchant complaint actions

11/20/2011: ATTENTION: Dear advertisers, we are having problems with our bank and our accounts were suddenly frozen. We're forced to temporarily stop accepting OEM traffic.


1/23/2012 Remark by leading affiliate: “The sun is setting on the OEM era”
Today

- OEM software market has been **decimated**
  - 90% of programs have folded
  - New startups (softbuy) shut down quickly

- Affiliates still operating won’t sell Microsoft software
The pharma story

- Much more developed ecosystem
- Intervention less focused, less comprehensive, less follow up
- Still significant impact...
Dear webmasters,

Due to the recent developments which led to all our bank and processing accounts being jeopardized, we have to inform you, that functioning of the Medinc partnership program will be discontinued, as no reliable solution has been found to keep it working, and the debts to suppliers and partners keep increasing.

We were happy to work with all of you, and we are very sorry that we can't cooperate with you anymore within this project.

If we manage to find a reliable processing solution to resume working, all webmasters will receive an email notification sent to the address submitted during registration.
Dear Partners,

As you may have noticed, in the last couple of days we've had problems with processing. We don't have a solution yet, and there is no concrete time when it will be resolved.

From this point forward, GlavMed is switching to a "PAUSED" mode. No new orders will be processed until the processing issue is resolved.

We urge you to temporarily switch your traffic to other shops/projects.
Hello all!

I would like to notify the advertisers of the OXOnetwork affiliate program that I have made the decision about its closure.

...
To all Cashadmin affiliates, .... RX industry is under attack from all sides. Recently, we have lost our credit card processing abilities several times, and it has come to the point where we are losing more money processing orders than we are getting from the orders themselves. The industry has become impossible to manage and maintain. Cashadmin has closed its sites...
“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).”
Pharma programs accepting US Visa purchases in 2011
Pharma programs accepting US Visa purchases today
Our research is driven by two beliefs

- Effective intervention will require reasoning about the economic/social structure of our adversaries
- This reasoning should be informed by empirical measurement data and fieldwork

This research agenda is both achievable and has the opportunity for major impact (both for research and the real world)