The Economics of Attack and Defense : Spam Ecosystem

Jeffrey Avery
Dependable Computing Systems Lab (DCSL)
Purdue University

PURDUE UNIVERSITY

Papers Presenting

- Click Trajectories: End-To-End Analysis of the Spam Value Chain (S&P 2011)
  - Main idea: quantify resources used to monetize spam
- Priceless: Role of Payments in Abuse-advertised Goods (CCS 2012)
  - Main idea: show undermining monetization of spam ecosystem is a viable defense

PURDUE UNIVERSITY

Outline

- Background
- Trajectory stages of spam
- Trajectory data
- Trajectory analysis
- Trajectory pressure
- Trajectory affiliated response
- Priceless data
- Priceless analysis
- Priceless pressure
- Priceless affiliate response
- Overall conclusion
- Questions

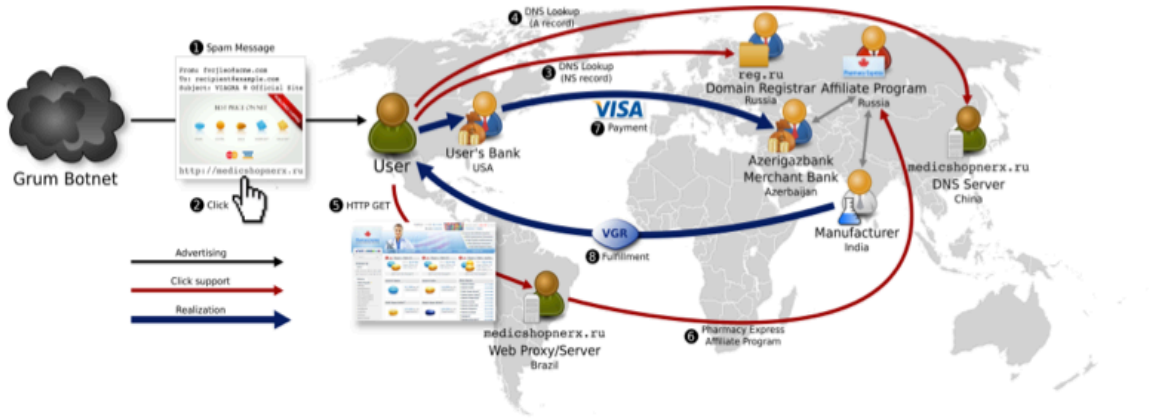
Background

- Spam enterprise is more than emails
  - Spam chain comprised of registrar, domain, servers, hosting, affiliate program, payment processing, fulfillment
- Spam Ecosystem
  - Affiliated Marketing
    - Affiliate program and sponsor
    - Merchant account
    - Onsite vs. offsite payment
  - Open loop payment/banking
  - Banking relationship

Trajectory Stages of Spam

- Advertising
  - Reaching the masses
  - Much work on defense has been done in this arena
    - Filters and browser toolbars
- Click support
  - Pressing a link and getting to a website
  - Must pressure registrars to impact domains used
- Realization
  - Customer wants to purchase some product and affiliate program acquires customer's payment to fulfill request

Trajectory Spam Stages Visualized



Trajectory Data Collection

- URL feeds
- Feed parsers extract URLs from raw spam feed and botnet-harvested spam
- Crawl websites
  - DNS crawler enumerate resource records of URL
  - Web crawler visit URL and record HTTP interactions
- Pharmaceutical, replica and software sites

Trajectory Organization of Data

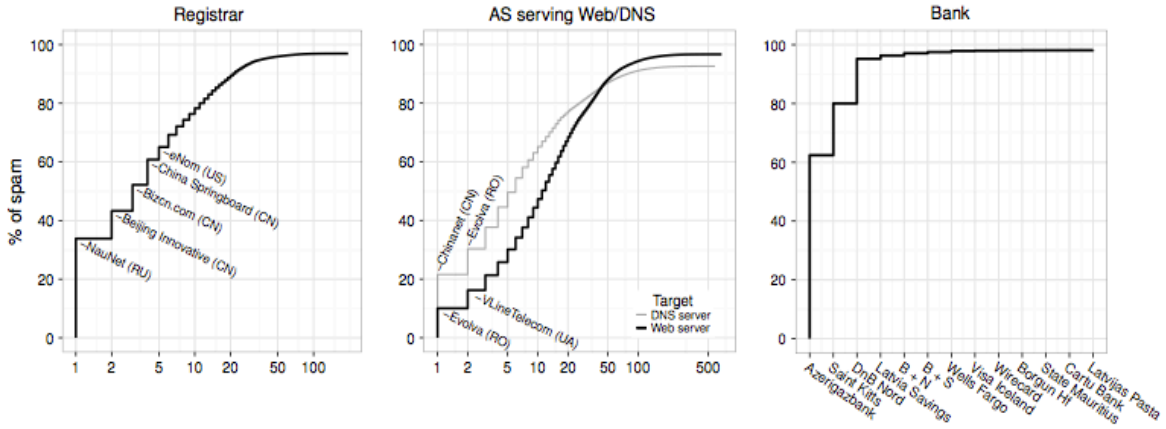
- Content clustering
  - Match websites with similar structure
- Category tagging
  - Place site in a category of pharmaceutical, software or replica
- Program tagging
  - Determine which affiliate program a site belongs to
  - Use RegEx to match structure of site against program specific storefront templates/brands
  - Use operational modes on sites to tag as well

Trajectory Analysis

- Redirection by a third of the websites
- 2 registrars serve domains for over 20 of the affiliate programs
  - 80 registrars serve domains for just one affiliate program
- 2 ASes host DNS servers for over 20 programs
  - 350 host DNS servers for a single affiliate program
- 9 ASes host web servers for over 20 programs
  - 450 host web servers for a single affiliate program
- 3 Banks provide services to 95% of programs

PURDUE UNIVERSITY

Trajectory Graph Analysis



PURDUE UNIVERSITY

Trajectory Pressure

- Block advertising
  - Filtering and toolbars
- Disrupt click support
  - Registrar suspend domains
  - Shut down associated hosts in an address space
- Disrupt merchant and payment step
  - Aggressively pursue spam related merchant accounts
  - Banks refuse to settle certain MCC transactions

Trajectory Affiliate Response

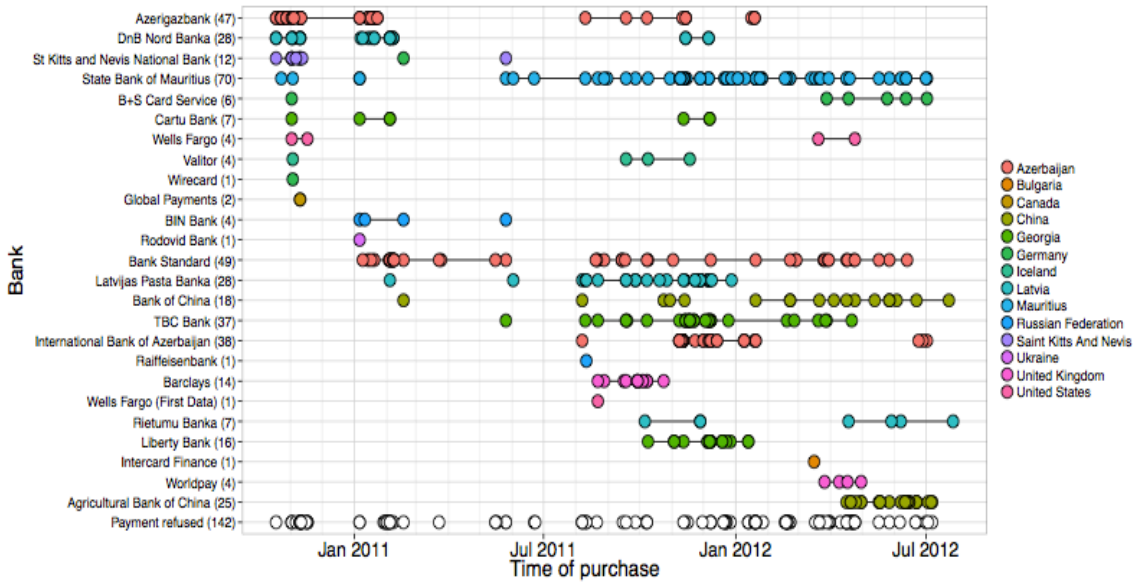
- Change hosting services
  - Low cost to the program as many hosting services and compromised servers
- Change domain name
  - Low cost to the program when bought in bulk
  - Registrars and registries move slowly
- Change bank
  - High cost to the program as very few banks process “high risk” transactions

Priceless Data

- Sites hosting spam pages
  - Domain Knowledge
    - Used classifier to categorize sites by looking at website template
  - Underground forums
    - Get template from here
  - Collaborations
    - XyliBox, criminal and civil investigation community
  - Placing orders (all are Visa transactions)
    - Placed around one order a month for each affiliate program they identified (40 programs)
- Pharmaceutical and OEM (software) sites

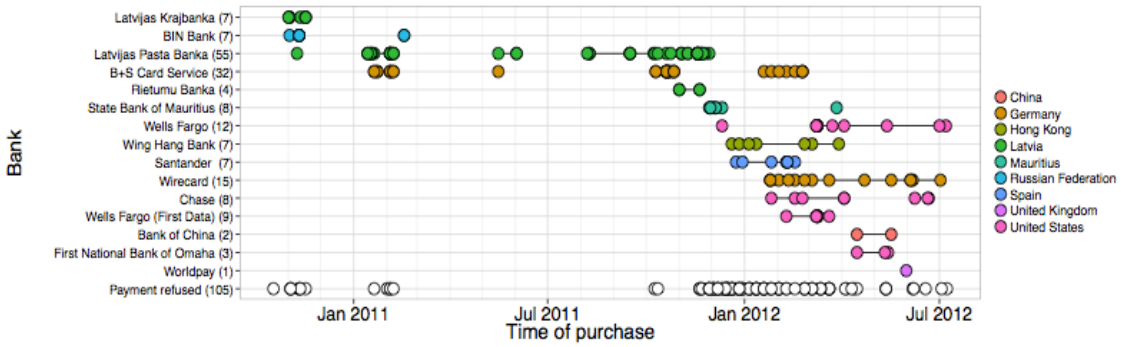
Priceless Analysis

- 25 banks used for pharmaceuticals
  - There are 12 main banks used



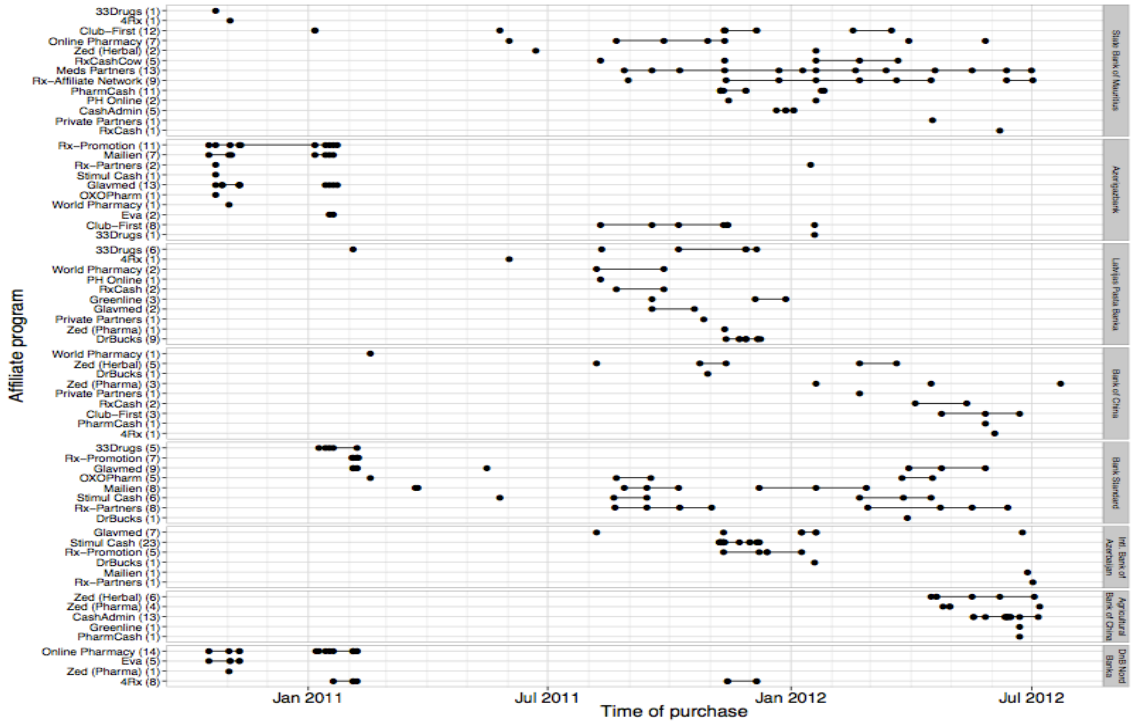
Priceless Analysis Continued…

- 11 total banks used for software
  - 4 main banks used



PURDUE UNIVERSITY

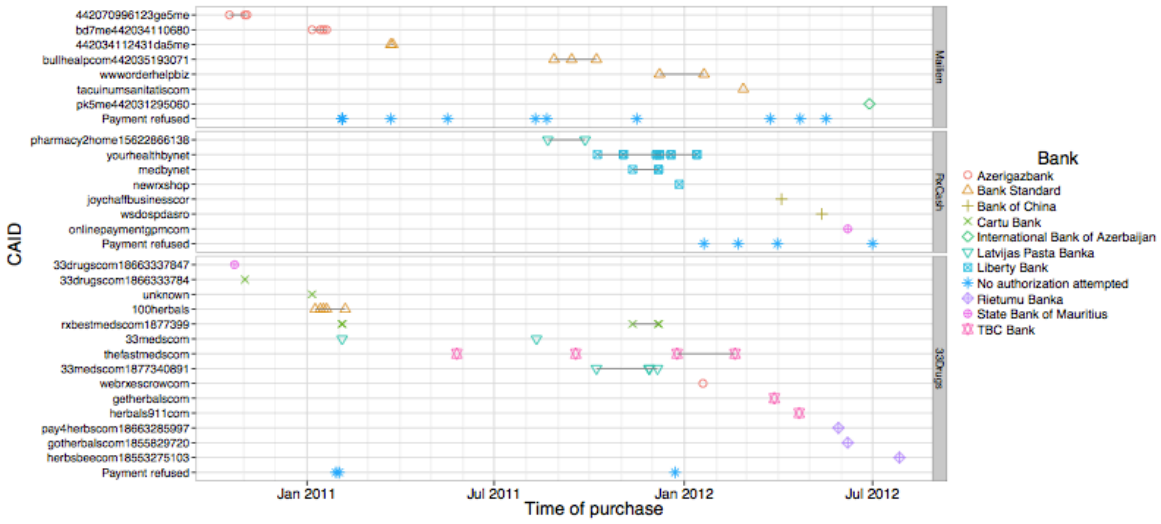
Priceless Analysis: Bank Use



PURDUE UNIVERSITY

Priceless Analysis: Terminals

- Terminals identify a merchant account



PURDUE UNIVERSITY

Priceless Pressure

- From the graphs policy and bank changes impact spam ecosystem
  - Applying outside pressure on banks to monitor and pursue these accounts aggressively
    - Chargeback rate
    - Complaints

PURDUE UNIVERSITY

Priceless Affiliate Response

- Affiliate programs adapt to these defenses
  - Phone verification
  - Document customer information and verify
  - Blacklist “high risk” customers
  - Complaint bypass
    - Remove product
    - Change name
  - Evasion using different Merchant Category Code (MCC)
  - US banks
  - Alternate payment process
  - Change terminals

Conclusion

- Complaints highly correlated with program moving to a new bank or stopping program completely
  - Causes opportunity loss during switch and hold back fee for leaving bank
- Banks taking action against spam will make the business very difficult
  - No bank means no money
  - US banks do actively detect these types of accounts
- MasterCard doesn’t cooperate/associate with these types of merchant accounts

Questions

- Are the pharmaceutical drugs that get delivered real? If so, how do the sponsor gain access to these drugs? Does this make them drug dealers and thus have legal implications?
- What other products can be sold through spam?
- Would allowing spam to get through filters and allowing users to "purchase" good, but stopping the final transaction from occurring be a good defense? Should more effort be thrown at building up the detection of spam activity at the banking level?
- Why does Visa deal with these types of transactions but MasterCard doesn't?
- Can behavior analysis on accounts at banks help to detect spam merchant accounts?
- Any more questions?

Bibliography

1. Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker, and Stefan Savage. 2012. Priceless: the role of payments in abuse-advertised goods. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 845-856. DOI=10.1145/2382196.2382285 http://doi.acm.org/10.1145/2382196.2382285

2. Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. 2011. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In Proceedings of the 2011 IEEE Symposium on Security and Privacy (SP '11). IEEE Computer Society, Washington, DC, USA, 431-446. DOI=10.1109/SP.2011.24 http://dx.doi.org/10.1109/SP.2011.24