CMSC 33250: Graduate Computer Security

Lecture 2: Cybercrime Ecosystems

Grant Ho, Fall 2023

(Some slides borrowed & adapted from Stefan Savage & Vern Paxson)

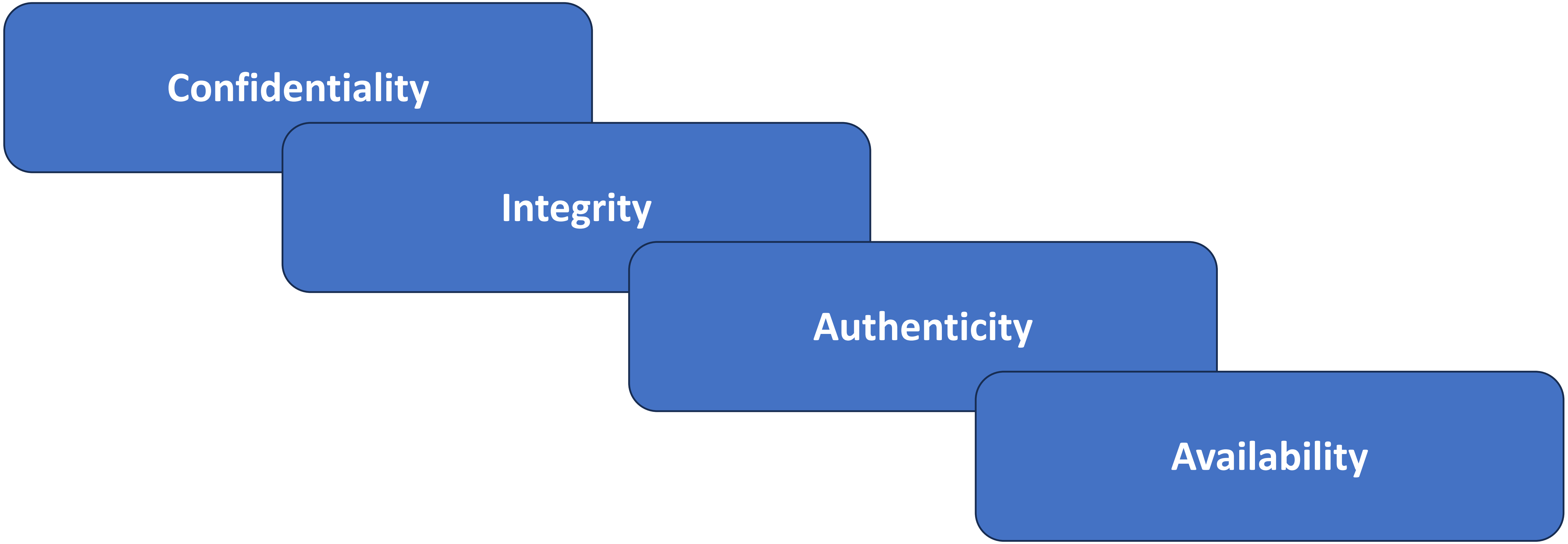
Introductions

- Your Name
- Program
- Year in program
- Lived in a place where it snows?
- Research Interests or Fun Fact

I am terrible at remembering names… It will take me a couple of classes.

Overview: Cybercrime

Classical (Technical) View of Security



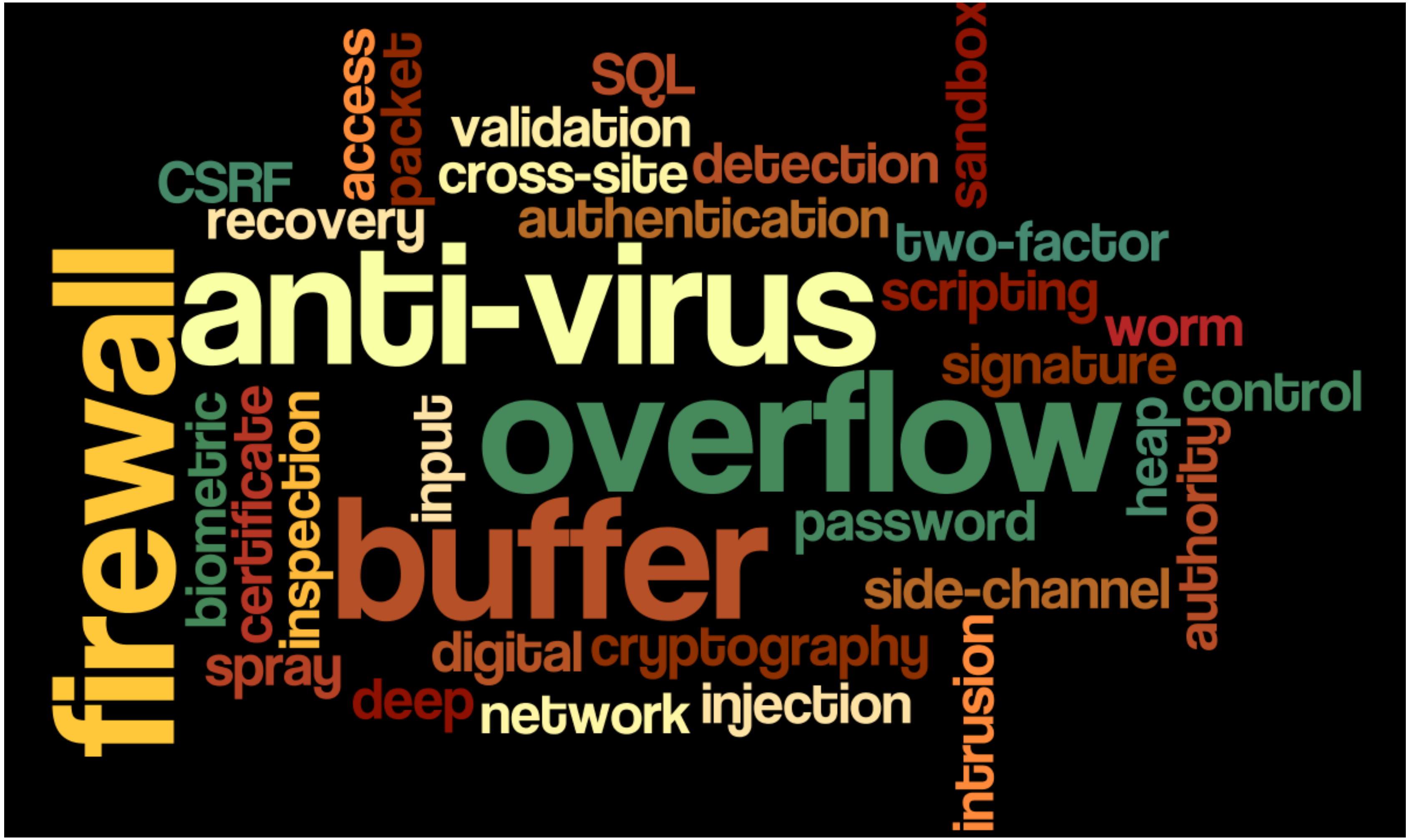
Confidentiality

Integrity

Authenticity

Availability

Classical (Technical) View of Security



Complementary Viewpoint

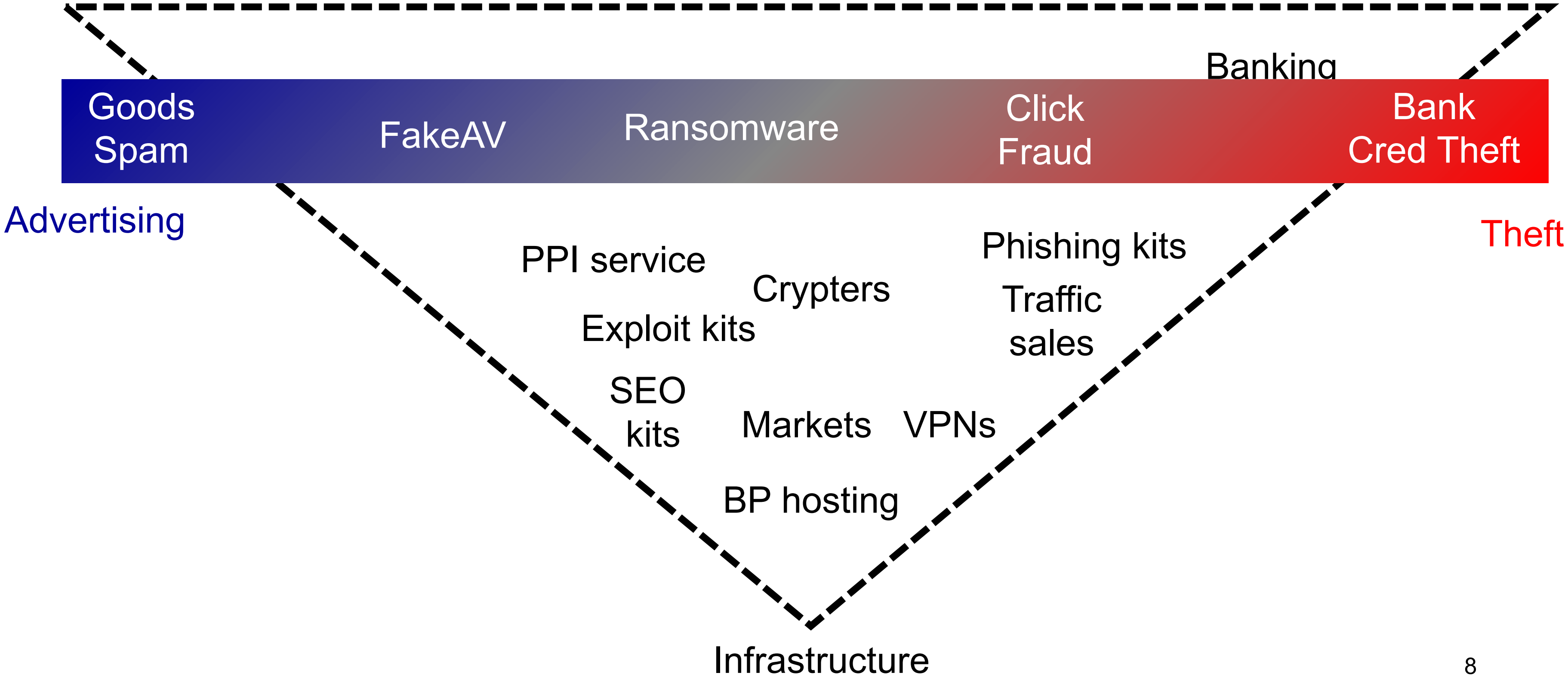
- There is a broader socio-economic context

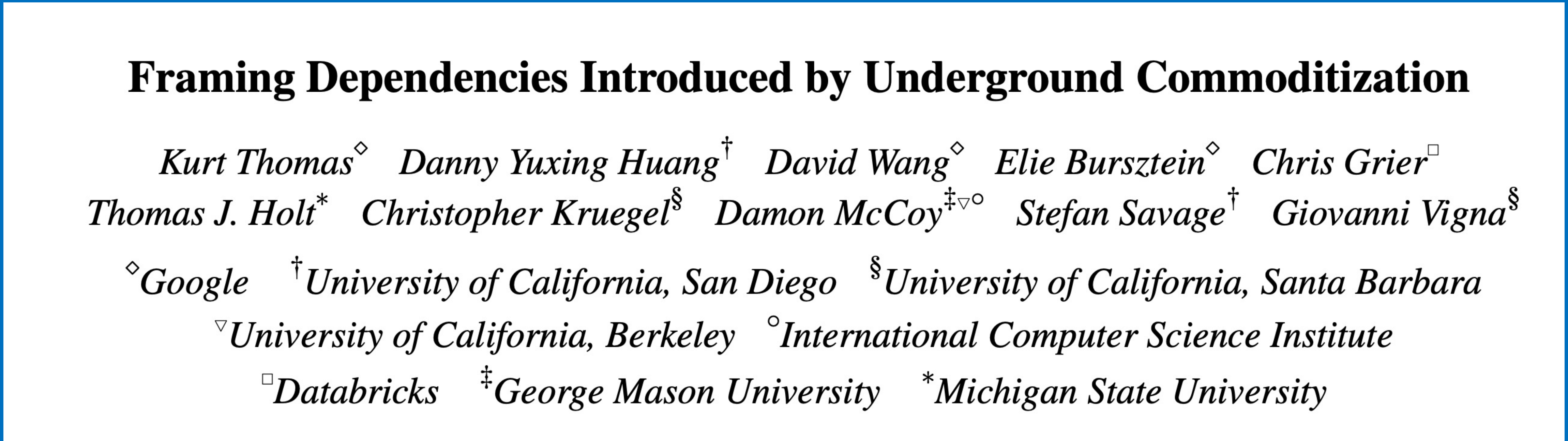
- Actors
  - Adversaries
  - Victims
  - Defenders
- Incentives/Costs
- Capabilities
- Relationships

- Conflict may be **mediated** by computers, but driven by social, political and **economic issues**
- To make good security decisions you need to understand the ecosystem

Structure & Economics of Cybercrime

Lots of pieces: how do they fit together and how is money made?





Framing Dependencies Introduced by Underground Commoditization

Kurt Thomas[◇] *Danny Yuxing Huang*[†] *David Wang*[◇] *Elie Bursztein*[◇] *Chris Grier*[□]
Thomas J. Holt[*] *Christopher Kruegel*[§] *Damon McCoy*[‡▽○] *Stefan Savage*[†] *Giovanni Vigna*[§]

[◇]*Google* [†]*University of California, San Diego* [§]*University of California, Santa Barbara*
[▽]*University of California, Berkeley* [○]*International Computer Science Institute*
[□]*Databricks* [‡]*George Mason University* [*]*Michigan State University*

What is the Problem?

Systemization of Knowledge (SoK) papers: expanded literature review

Problem Space: Understand the structure of the cybercrime ecosystem

Goal: Synthesize existing literature into a conceptual framework that

1. Helps us understand all the components of cybercrime ecosystem
2. Identifies high priority areas for interventions and future research

Structure of Underground Economy

- **Profit Centers:** activities that extract money from a victim

- **Support Centers:** activities that help acquire victims for profit centers

- **Payment Infrastructure:** services for sending/receiving money

Profit Centers

Input: Given user viewing traffic, compromised credentials/accounts, and/or compromised devices,

Output: Convert into money

- Spam
- Scareware
- Ransomware
- Click Fraud
- Bank / CC Theft

Support Centers

Services & Infrastructure to acquire users / accounts / machines ***at scale***

Machines

- Creating & selling exploits
- Pay-per-install: selling direct access to compro. machine
  - Droppers

Accounts

- Creating & selling fake accounts
- Selling compromised accounts
- Generating fake traffic

Network / Web Hosting

- Hosting network / web infrastructure
- Launching DoS attacks
- Providing web proxies
- SEO & Web cloaking

Human Services

- Human verification (CAPTCHAs, SMS)
- Content generation

Defenses & Interventions

What are some of the different defenses and interventions that the paper proposes to combat cybercrime?

Defenses & Interventions

- **Improve technical security** that prevents compromise of users/machines
- **Exhaust resources /stockpiles:** if we can’t prevent, then we can block or takedown compromised/malicious things
- **Payment interventions:** have banks, credit card companies, digital currency platforms prevent attackers from cashing out (or users from making payments)
- **Targeting actors:** arrest attackers

Interventions: Trade-offs

What are some of the challenges with the different approaches?

- Improve technical security
- Exhaust resources /stockpiles
- Payment interventions
- Targeting actors

Interventions: Trade-offs

What are some of the challenges with the different approaches?

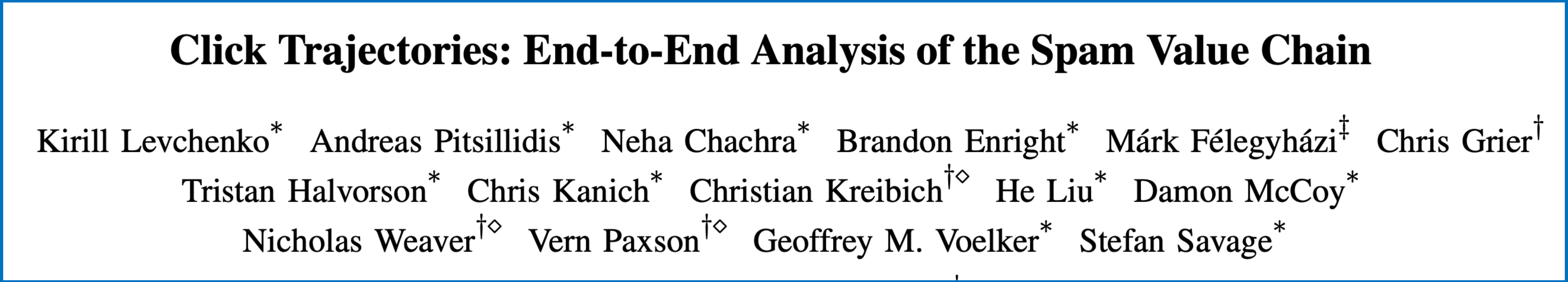
- **Improve technical security**: perfect security unattainable, will always be some attack/insecurity that exists
- **Exhaust resources /stockpiles**: a lot of resources are cheap & easy to migrate/acquire (IP addresses, domain names, etc.)
- **Payment interventions:** requires sustained policy pressure & cryptocurrencies may pose challenges
- **Targeting actors**: new actors emerge to fill void & legal jurisdiction challenges

Future Directions: Open Challenges that Remain?

1. Accurately estimating the revenue of different forms of abuse (profit centers)

2. Don’t have a good way to understand true value & ROI of different support center resources

3. Lack good data on long-term effect of different interventions



Click Trajectories: End-to-End Analysis of the Spam Value Chain

Kirill Levchenko[*] Andreas Pitsillidis[*] Neha Chachra[*] Brandon Enright[*] Márk Félegyházi[‡] Chris Grier[†]
Tristan Halvorson[*] Chris Kanich[*] Christian Kreibich[†◇] He Liu[*] Damon McCoy[*]
Nicholas Weaver[†◇] Vern Paxson[†◇] Geoffrey M. Voelker[*] Stefan Savage[*]

Click Trajectories: The Problem & Paper Goals

- Key idea
  - Find “bottlenecks” in the full spam value chain
  - Place where intervention could be most effective
    - Eliminating resources has largest **impact on profitability**
    - Fewest alternatives, **highest switching cost** for adversary

- Paper style: “Measurement Paper”
  - Methodology: data collection & cleaning
  - Evaluation: analysis techniques to draw conclusions/results
  - Contributions: new insights, methods/techniques, and/or datasets

Background: Affiliate Programs

Starting point: merchant who produces illicit good (counterfeit products & jewelry, off-market drugs/pharma, pirated software, etc.)

- Need to advertise lots of potential online customers to make $$$

But how do they acquire lots of online customers?

- Illicit goods, so can’t advertise traditionally
- Might not be tech savvy, so can’t/won’t figure out network + web hosting, evading blocklists, mass-mail around spam filters, etc.

Business Solution: Affiliate Programs

Background: Affiliate Programs

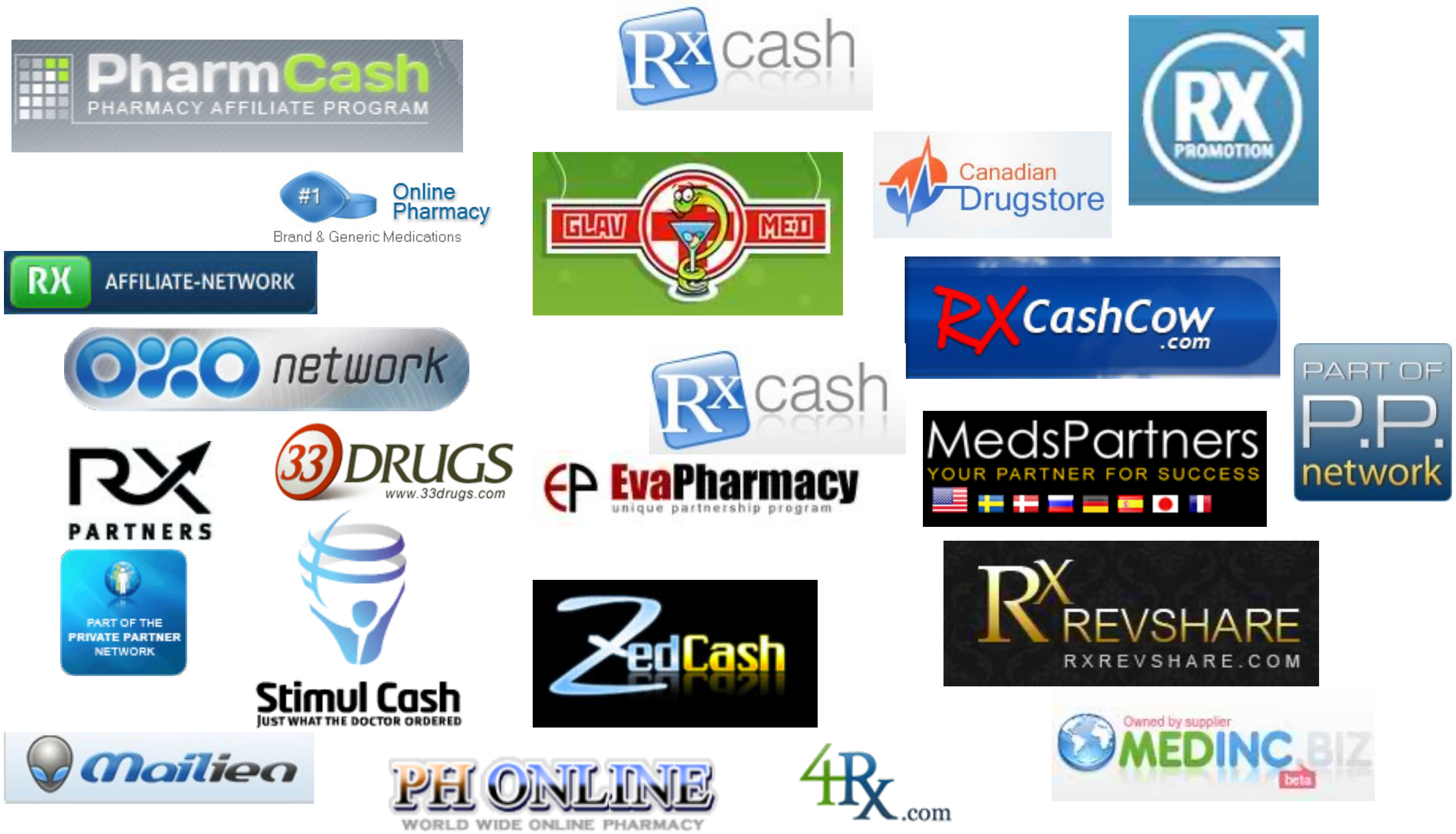
Merchant (Business sponsor) creates an Affiliate Program

- Fulfillment
  - Goods production & handling, drop shipping
- Customer service
- Payment services
  - Visa/MC – typically via third-party structure
- Content
  - Web page templates, advertising literature

Hire individual Affiliates to get user traffic to store (often including associated network/web infrastructure)

- Affiliates paid on commission basis (~40%)

Many Affiliate Programs Out There…

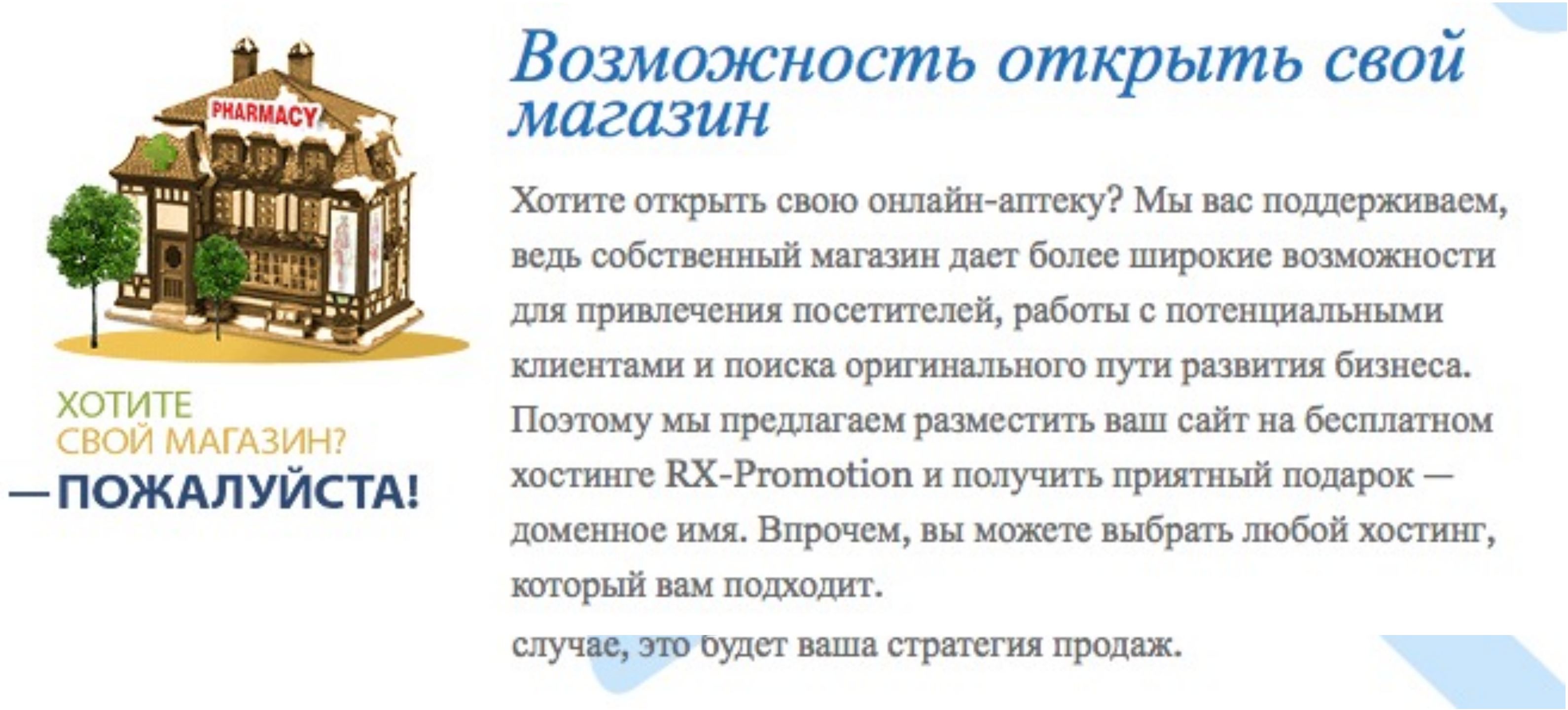


30-60% sale commissions

On-demand payments

Low drug prices

Run your own shop



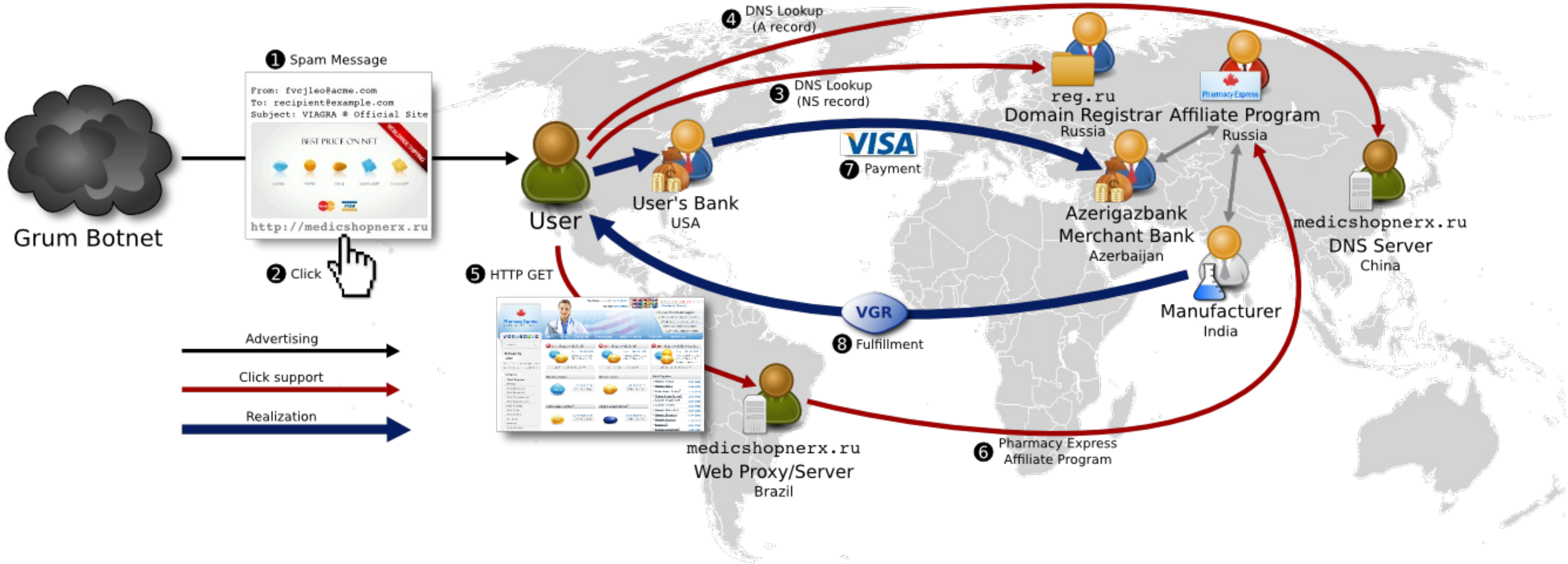
ХОТИТЕ СВОЙ МАГАЗИН?
—ПОЖАЛУЙСТА!

Возможность открыть свой магазин

Хотите открыть свою онлайн-аптеку? Мы вас поддерживаем, ведь собственный магазин дает более широкие возможности для привлечения посетителей, работы с потенциальными клиентами и поиска оригинального пути развития бизнеса. Поэтому мы предлагаем разместить ваш сайт на бесплатном хостинге RX-Promotion и получить приятный подарок — доменное имя. Впрочем, вы можете выбрать любой хостинг, который вам подходит.

случае, это будет ваша стратегия продаж.

Background: How spam-advertising works

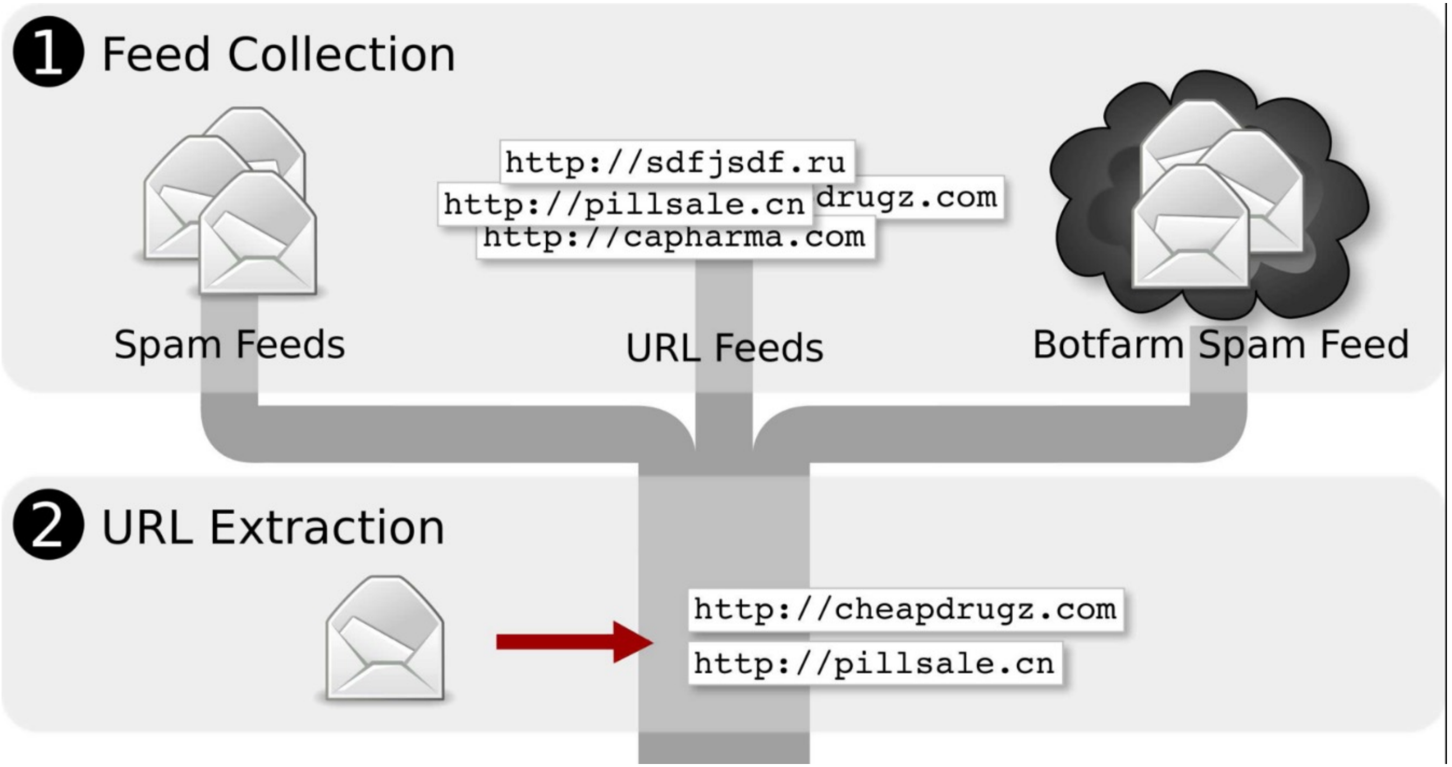


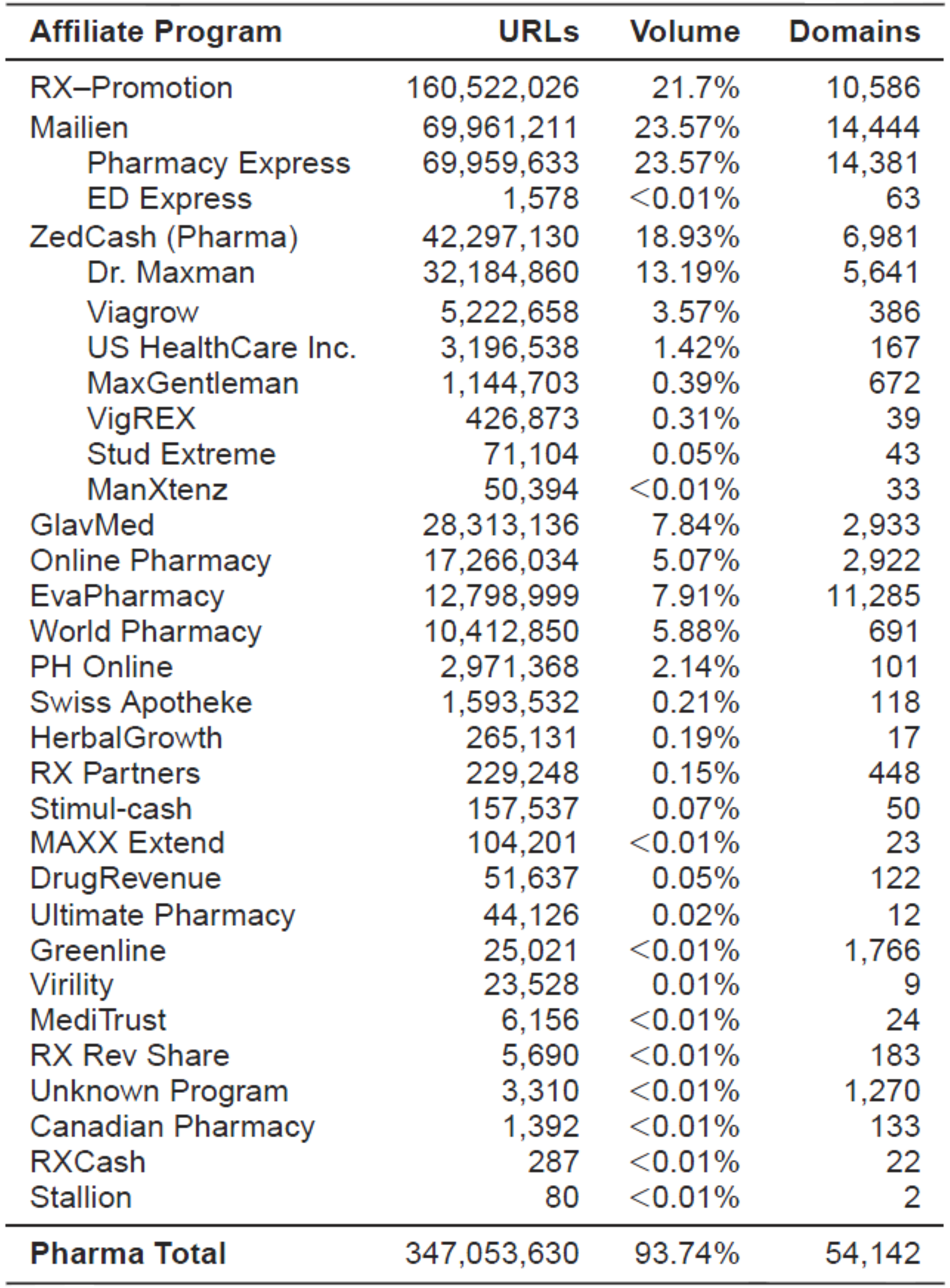
From: fvcjleo@acme.com
To: recipient@example.com
Subject: VIAGRA ® Official Site

http://medicshopnerx.ru

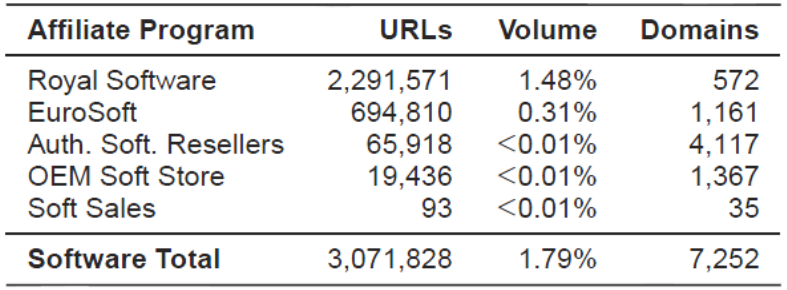
Goal: If we “snip” a link in this chain, which one would be the most disruptive for our least expenditure?

Methodology: Data Collection





Affiliate Program	URLs	Volume	Domains
RX–Promotion	160,522,026	21.7%	10,586
Mailien	69,961,211	23.57%	14,444
Pharmacy Express	69,959,633	23.57%	14,381
ED Express	1,578	<0.01%	63
ZedCash (Pharma)	42,297,130	18.93%	6,981
Dr. Maxman	32,184,860	13.19%	5,641
Viagrow	5,222,658	3.57%	386
US HealthCare Inc.	3,196,538	1.42%	167
MaxGentleman	1,144,703	0.39%	672
VigREX	426,873	0.31%	39
Stud Extreme	71,104	0.05%	43
ManXtenz	50,394	<0.01%	33
GlavMed	28,313,136	7.84%	2,933
Online Pharmacy	17,266,034	5.07%	2,922
EvaPharmacy	12,798,999	7.91%	11,285
World Pharmacy	10,412,850	5.88%	691
PH Online	2,971,368	2.14%	101
Swiss Apotheke	1,593,532	0.21%	118
HerbalGrowth	265,131	0.19%	17
RX Partners	229,248	0.15%	448
Stimul-cash	157,537	0.07%	50
MAXX Extend	104,201	<0.01%	23
DrugRevenue	51,637	0.05%	122
Ultimate Pharmacy	44,126	0.02%	12
Greenline	25,021	<0.01%	1,766
Virility	23,528	0.01%	9
MediTrust	6,156	<0.01%	24
RX Rev Share	5,690	<0.01%	183
Unknown Program	3,310	<0.01%	1,270
Canadian Pharmacy	1,392	<0.01%	133
RXCash	287	<0.01%	22
Stallion	80	<0.01%	2
Pharma Total	347,053,630	93.74%	54,142

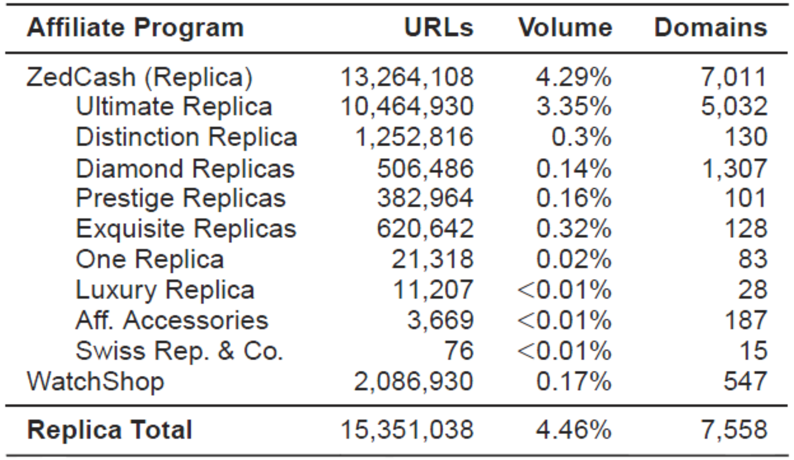


Affiliate Program	URLs	Volume	Domains
Royal Software	2,291,571	1.48%	572
EuroSoft	694,810	0.31%	1,161
Auth. Soft. Resellers	65,918	<0.01%	4,117
OEM Soft Store	19,436	<0.01%	1,367
Soft Sales	93	<0.01%	35
Software Total	3,071,828	1.79%	7,252

Looked at three categories:

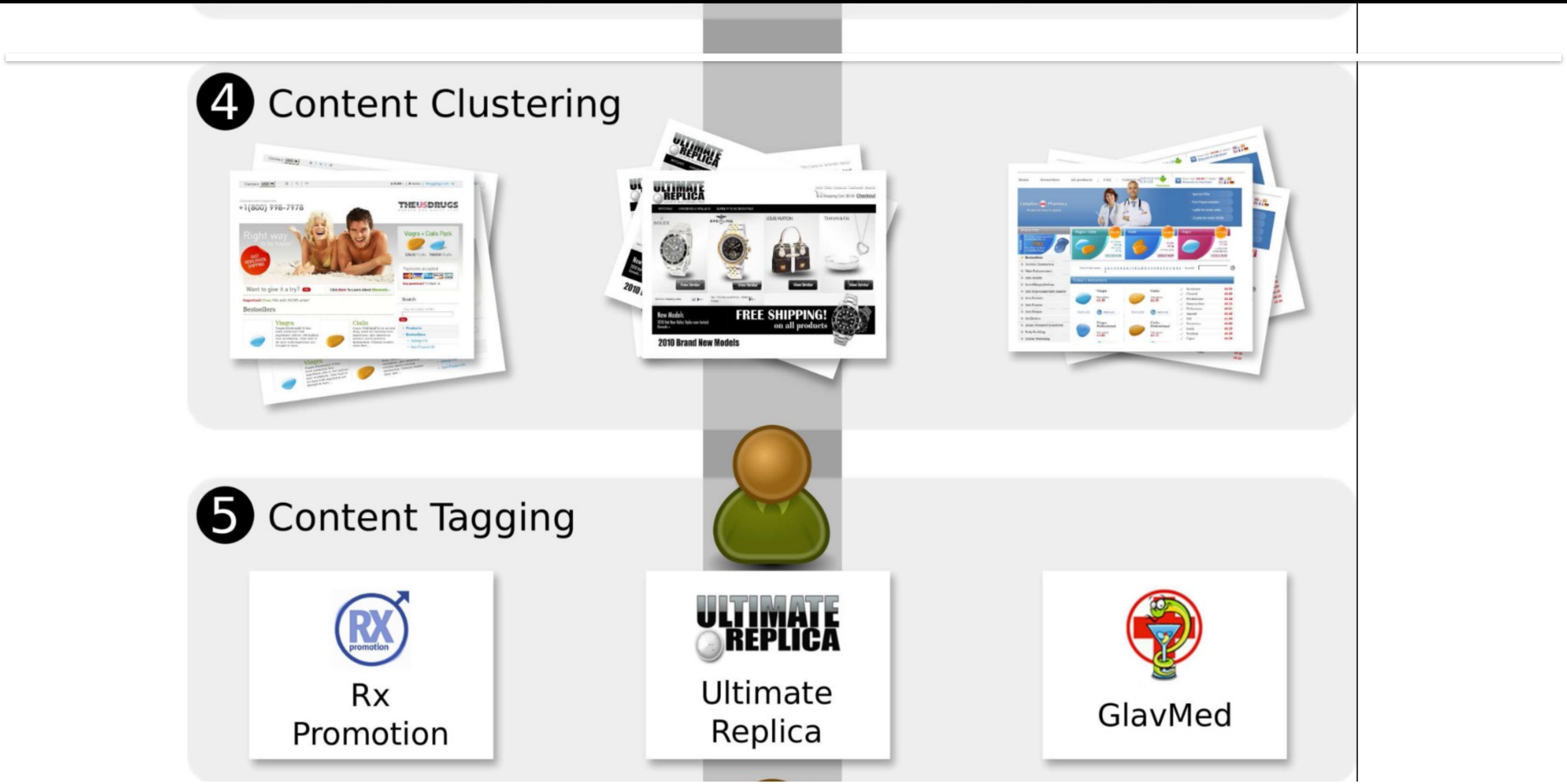
Pharma, Replica, Software

Cover all the major affiliate programs



Affiliate Program	URLs	Volume	Domains
ZedCash (Replica)	13,264,108	4.29%	7,011
Ultimate Replica	10,464,930	3.35%	5,032
Distinction Replica	1,252,816	0.3%	130
Diamond Replicas	506,486	0.14%	1,307
Prestige Replicas	382,964	0.16%	101
Exquisite Replicas	620,642	0.32%	128
One Replica	21,318	0.02%	83
Luxury Replica	11,207	<0.01%	28
Aff. Accessories	3,669	<0.01%	187
Swiss Rep. & Co.	76	<0.01%	15
WatchShop	2,086,930	0.17%	547
Replica Total	15,351,038	4.46%	7,558

Methodology: Data Collection



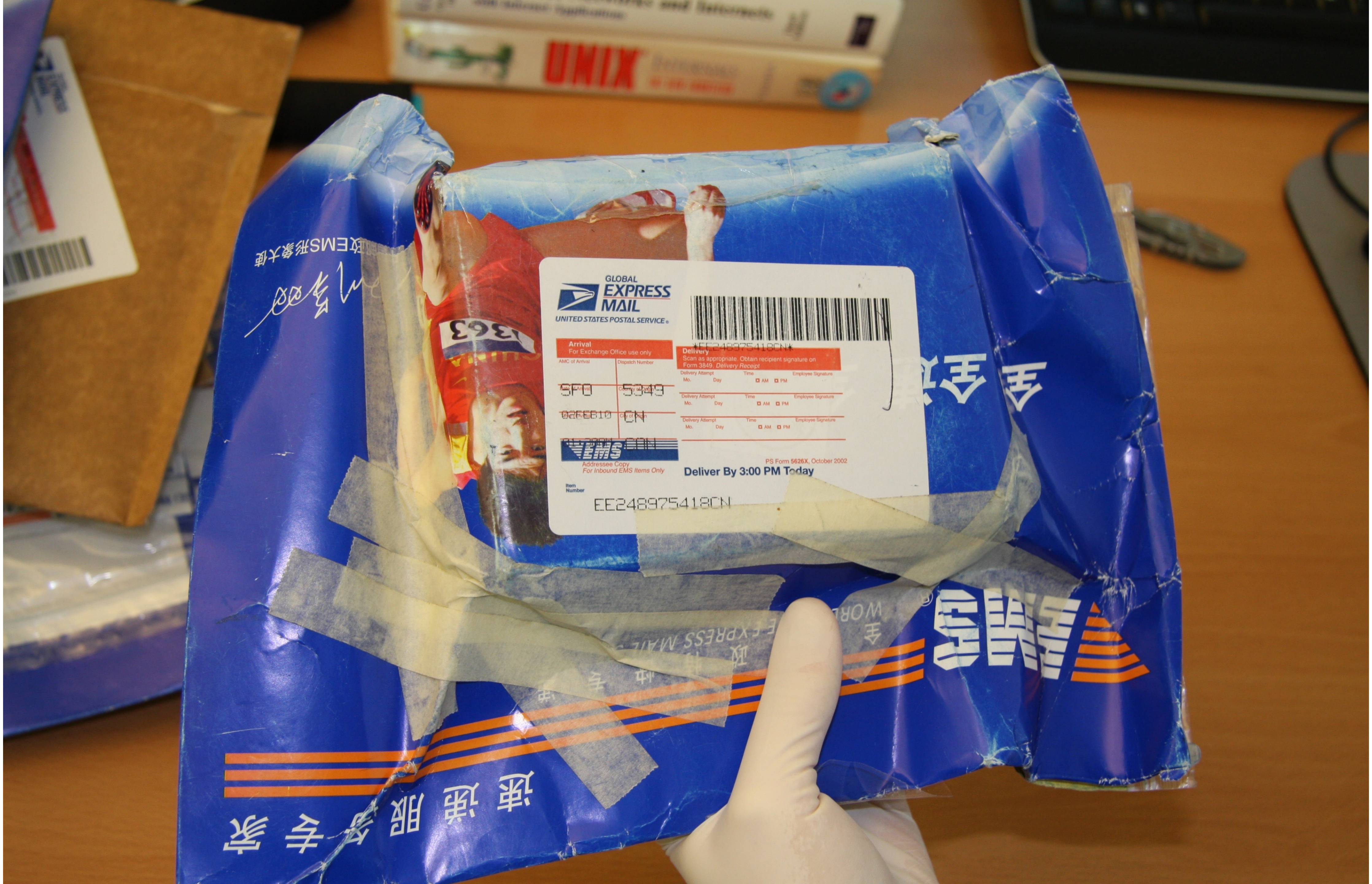
Methodology: What’s gained from purchasing?

Insight into **realization** phase

- Payment info (*via relationship with card issuer*)
  - **Bank Identification Number (BIN) of acquiring bank**
  - Card Acceptor ID (CAID) (MID + TID)
  - Merchant Category Code (MCC) (e.g., 5912=pharm)
- Fulfillment
  - Receiving anything?
  - Where shipped from?
  - Contents of order?

Director of purchasing

Project lead



GLOBAL EXPRESS MAIL
UNITED STATES POSTAL SERVICE®

EE248975418CN

Arrival
For Exchange Office use only

AMC of Arrival
Dispatch Number

Date of Arrival SFO
Country of Origin 5349

Time of Arrival 02FEB10
City of Origin CN

[illegible] CAN

EMS
Addressee Copy
For Inbound EMS Items Only

Delivery
Scan as appropriate. Obtain recipient signature on Form 3849, *Delivery Receipt*

Delivery Attempt Mo. Day Time □ AM □ PM Employee Signature

Delivery Attempt Mo. Day Time □ AM □ PM Employee Signature

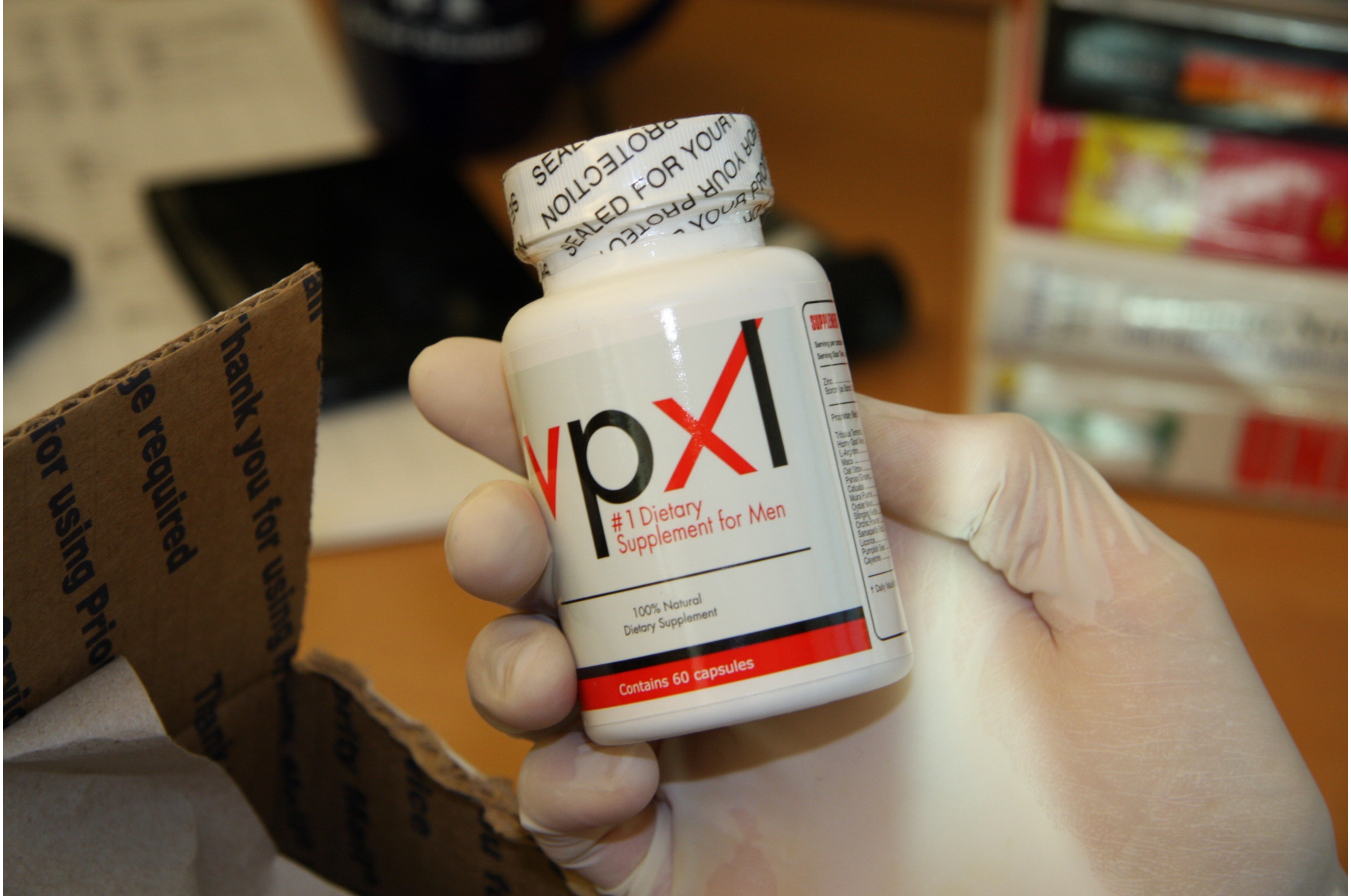
Delivery Attempt Mo. Day Time □ AM □ PM Employee Signature

PS Form 5626X, October 2002

Deliver By 3:00 PM Today

Item Number EE248975418CN

EXPRESS MAIL
DECLARATION EN DOUANE
SUPPLIERS
Road, Andheri (W).
MUMBAI 400 058
MEDICINE
Designation detaillee du contenu
Detailed Description of contents
Pill72
Cipla


SEALED FOR YOUR PROTECTION
vpXl
#1 Dietary Supplement for Men
100% Natural Dietary Supplement
Contains 60 capsules
thank you for using
ge required
for using Prio

20
10
30
40
50
ROLEX
OYSTER PERPETUAL DATE
16
SUBMARINER
1000ft=300m
SUPERLATIVE CHRONOMETER
OFFICIALLY CERTIFIED

Data Analysis & Results

- Consider interventions in:
  - Click Support
    - Registrar
    - DNS hosting
    - Web hosting
  - Realization
    - Payments

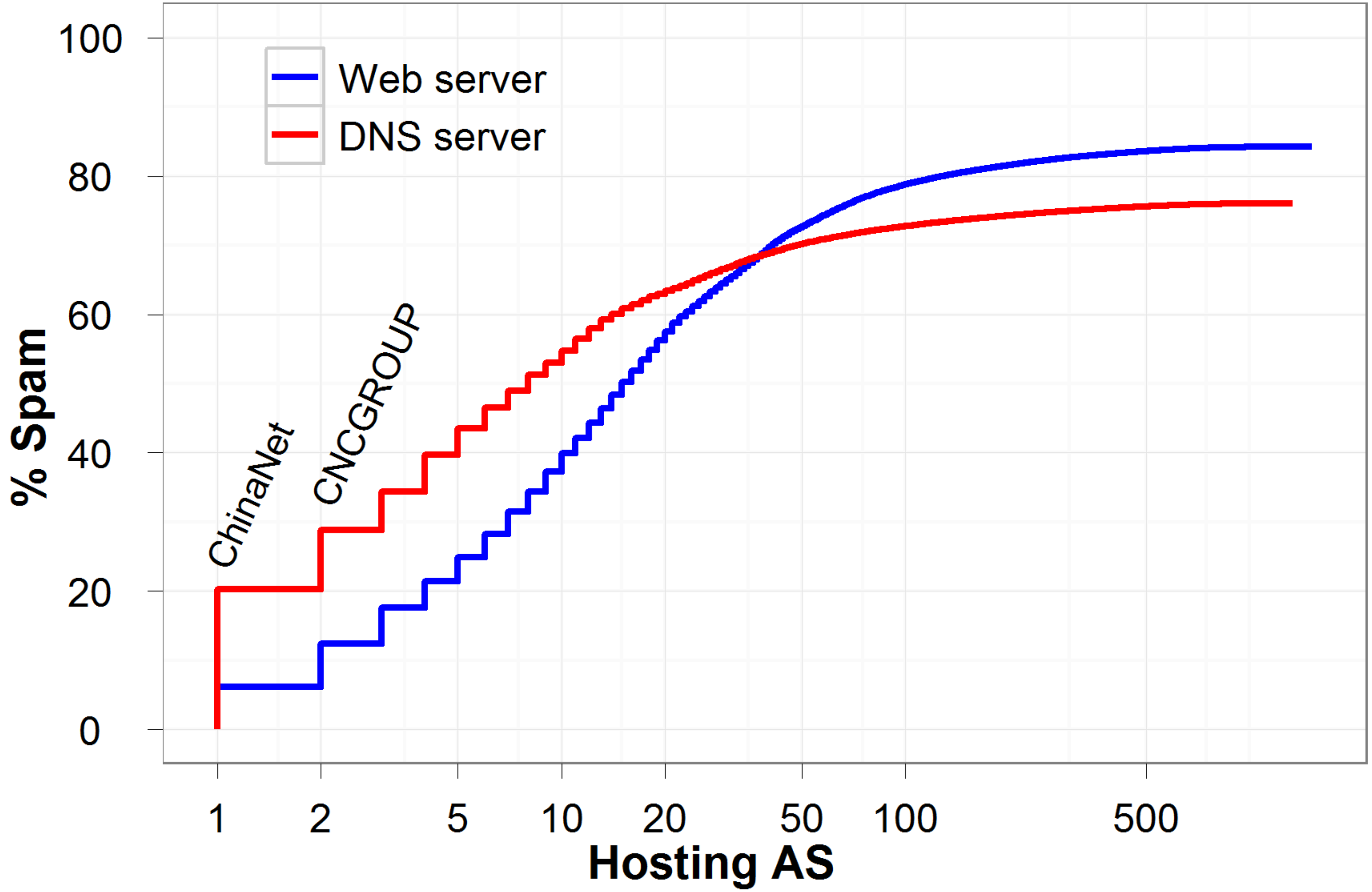
- Are there bottlenecks at any of these tiers?

Data Analysis & Results: Identifying Bottlenecks

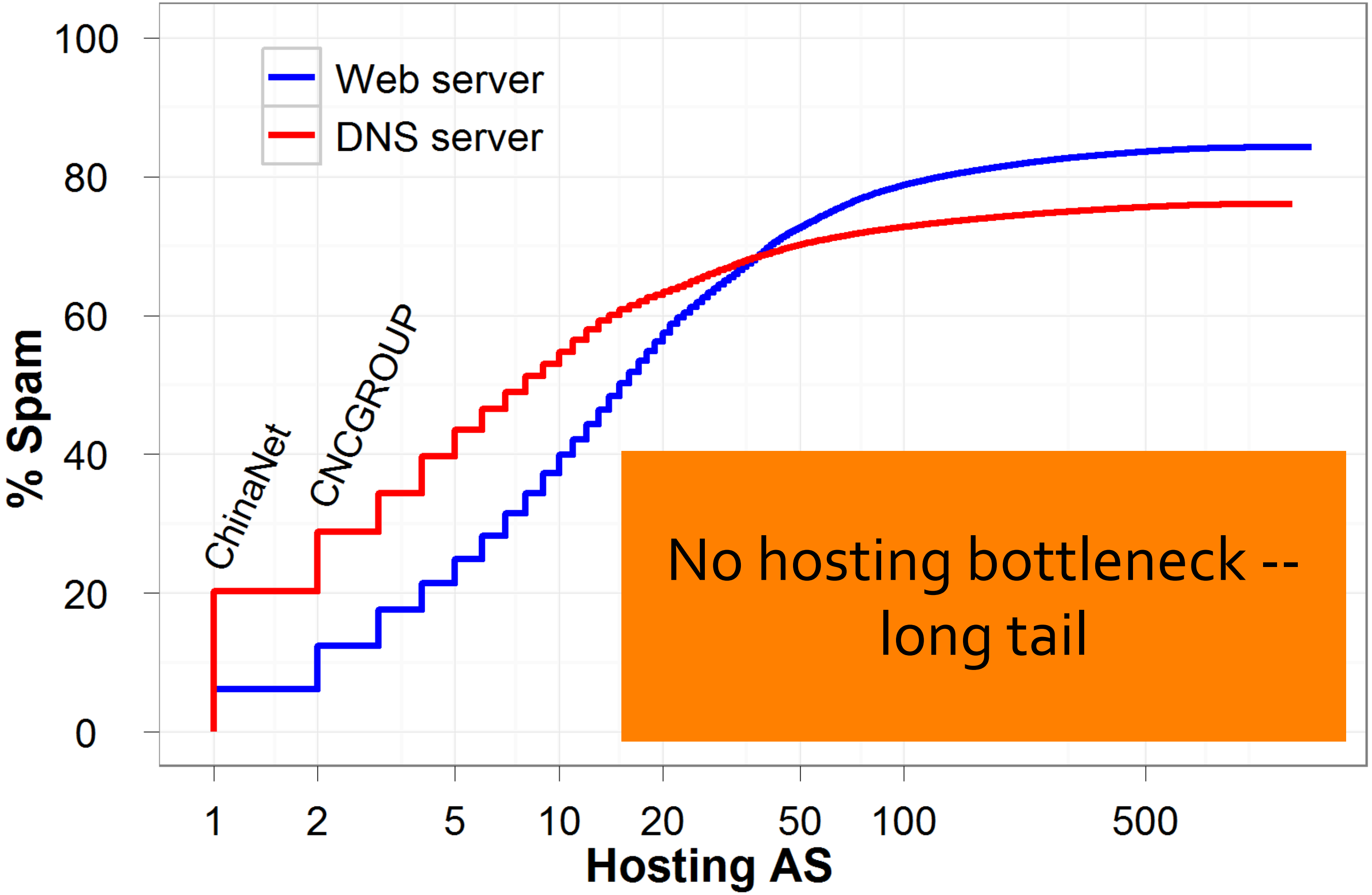
- Consider interventions in:
  - Click Support
    - Registrar
    - DNS hosting
    - Web hosting
  - Realization
    - Payments

- Analysis Criteria: What makes an effective bottleneck?
  - Scale of impact: how much spam affected?
  - Business impact to spammers: how painful / costly / hard to adapt?
  - Overhead of intervention: how difficult to implement?

Hosting Bottlenecks?

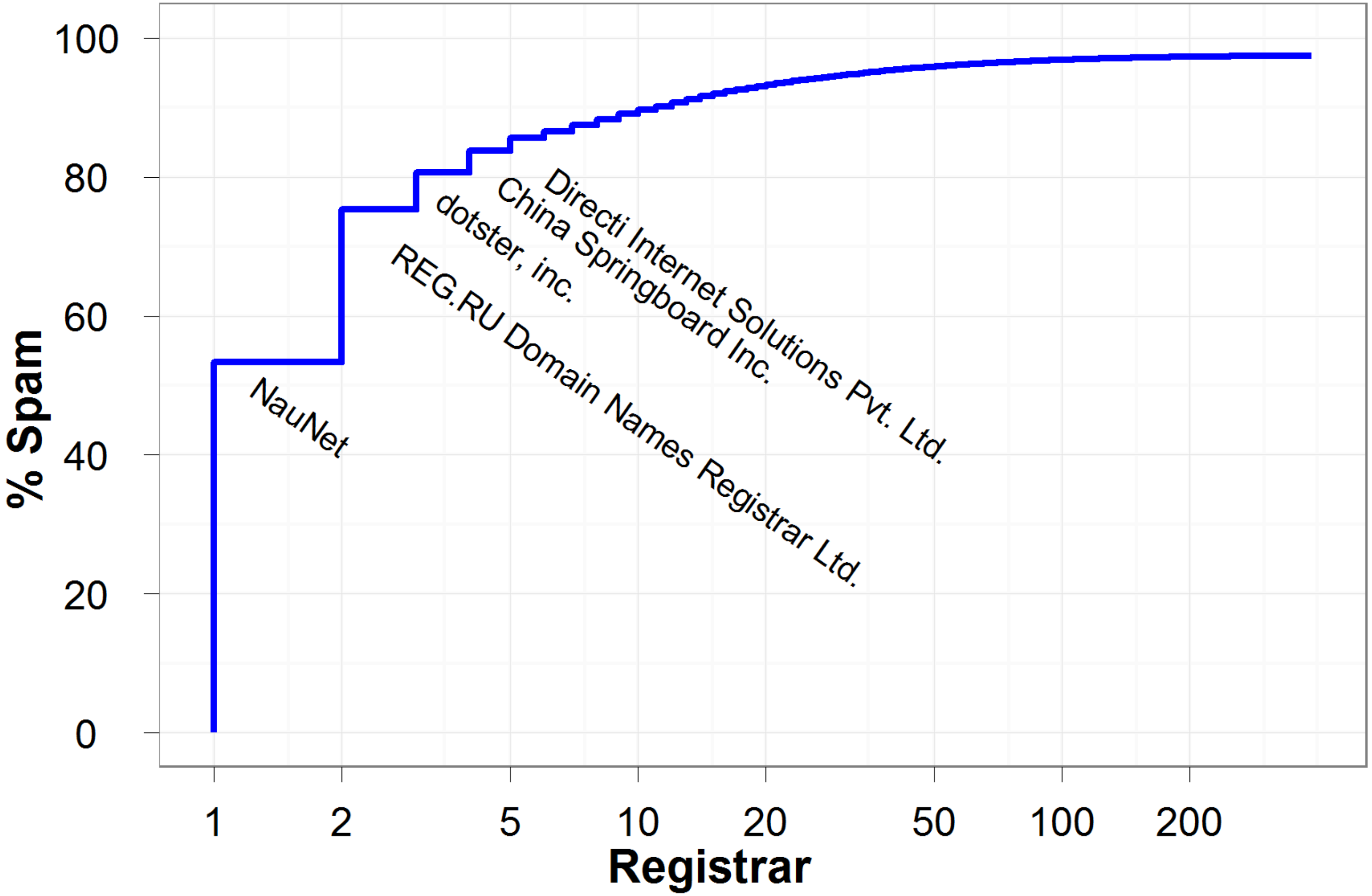


Hosting Bottlenecks?

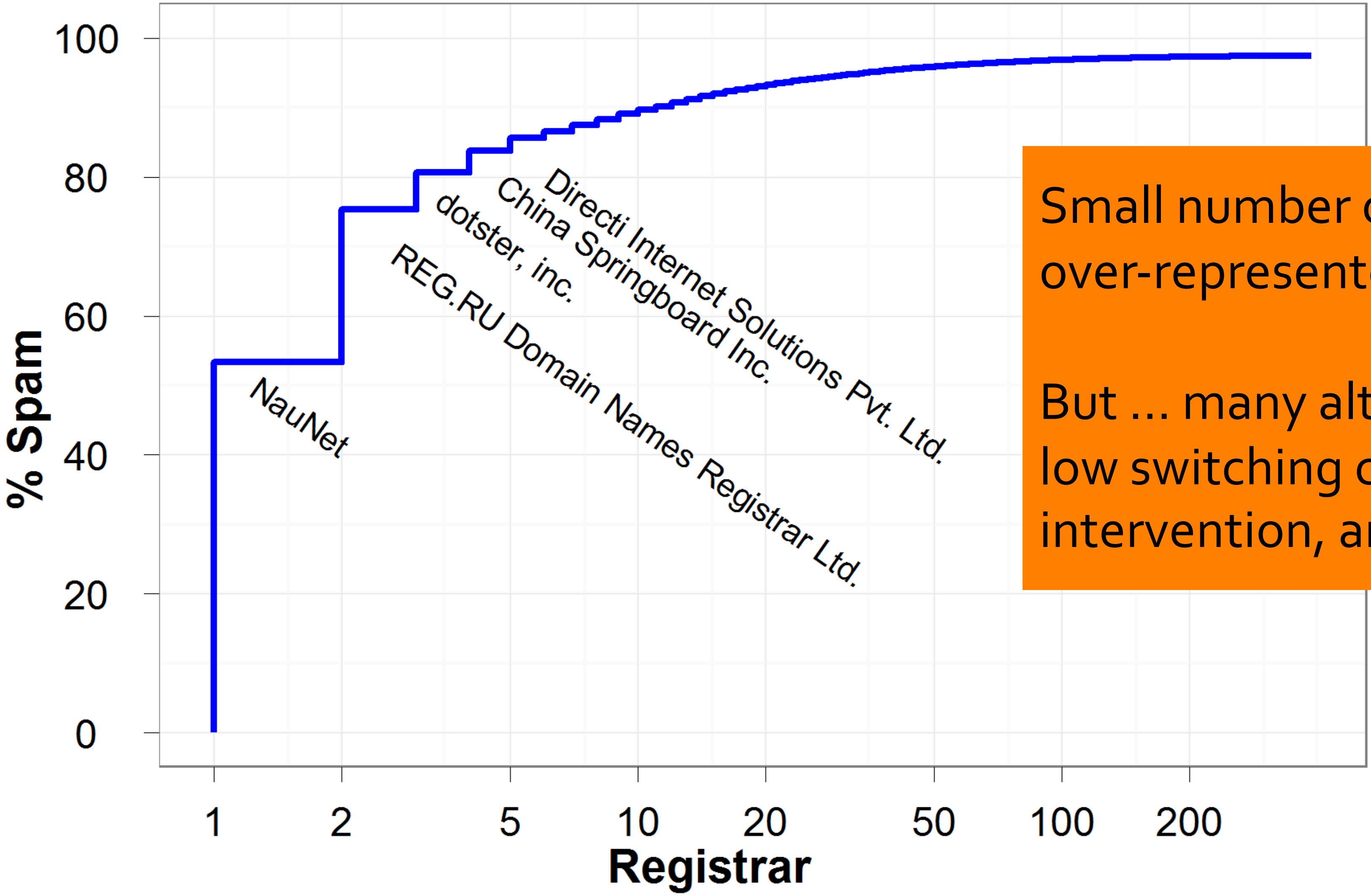


No hosting bottleneck -- long tail

Registrar Bottlenecks?



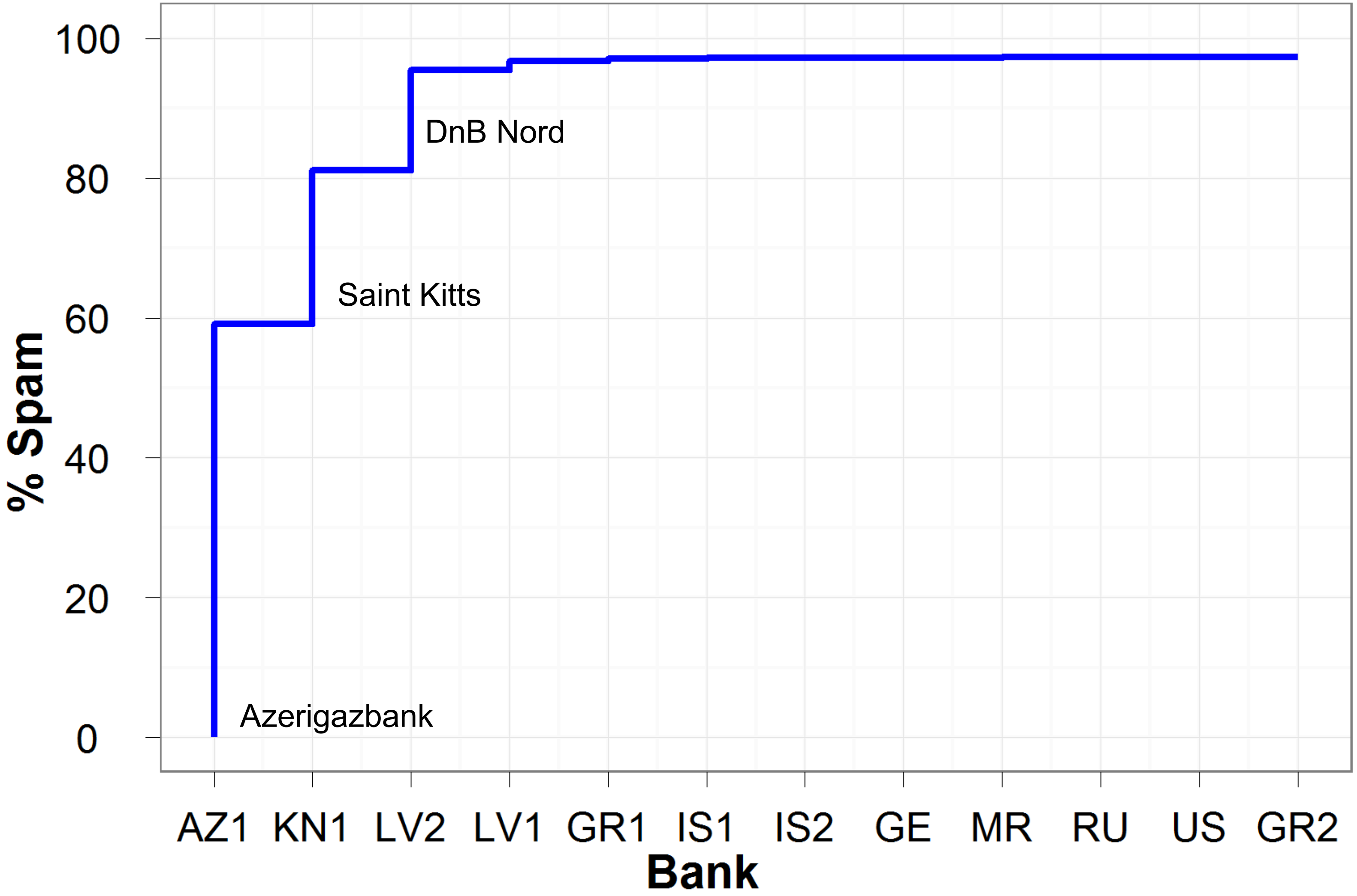
Registrar Bottlenecks?



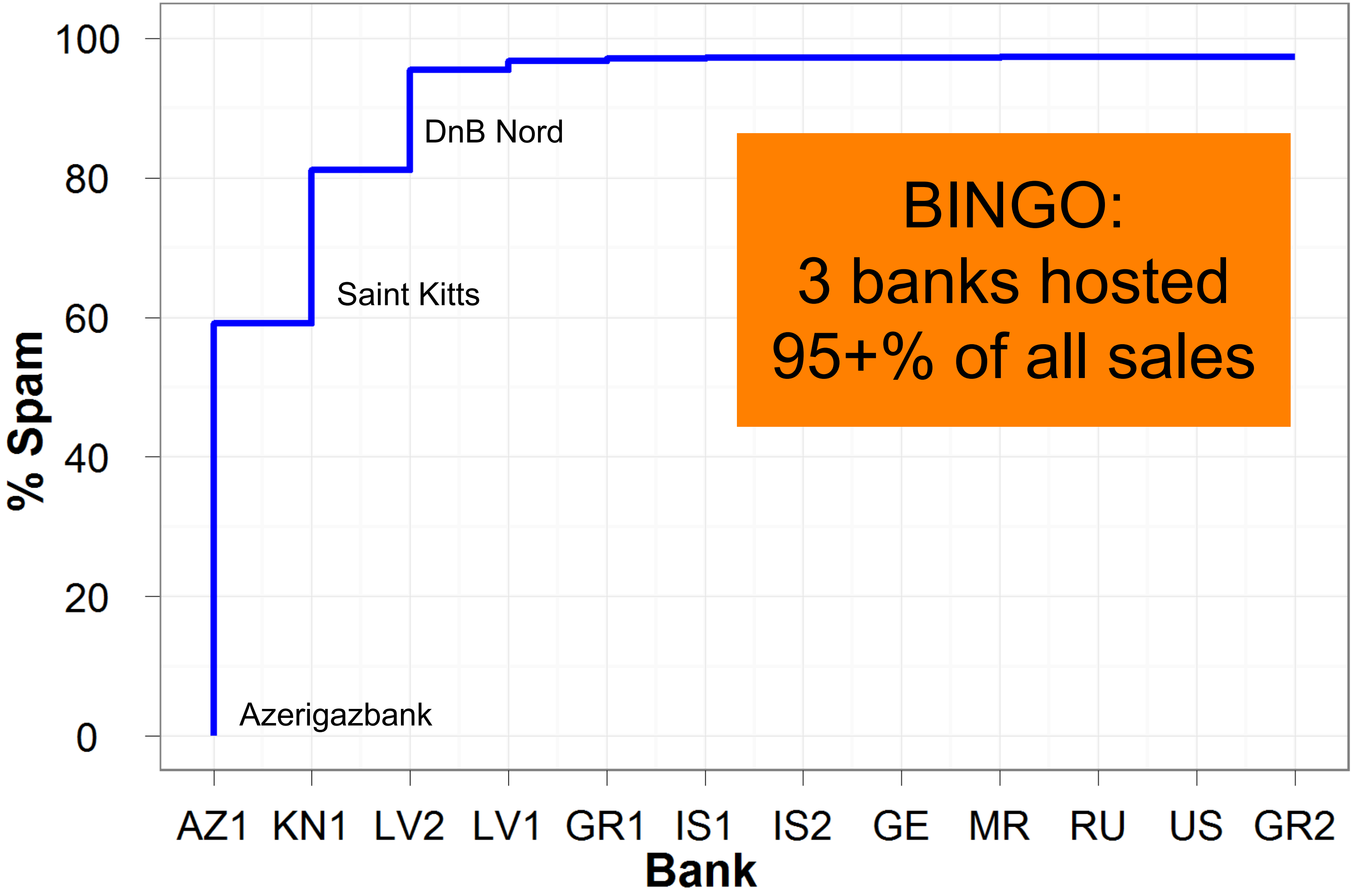
Small number of registrars over-represented in spam

But … many alternatives, low switching cost, slow intervention, and long tail

Payment (Merchant Bank) Bottlenecks?



Payment (Merchant Bank) Bottlenecks?

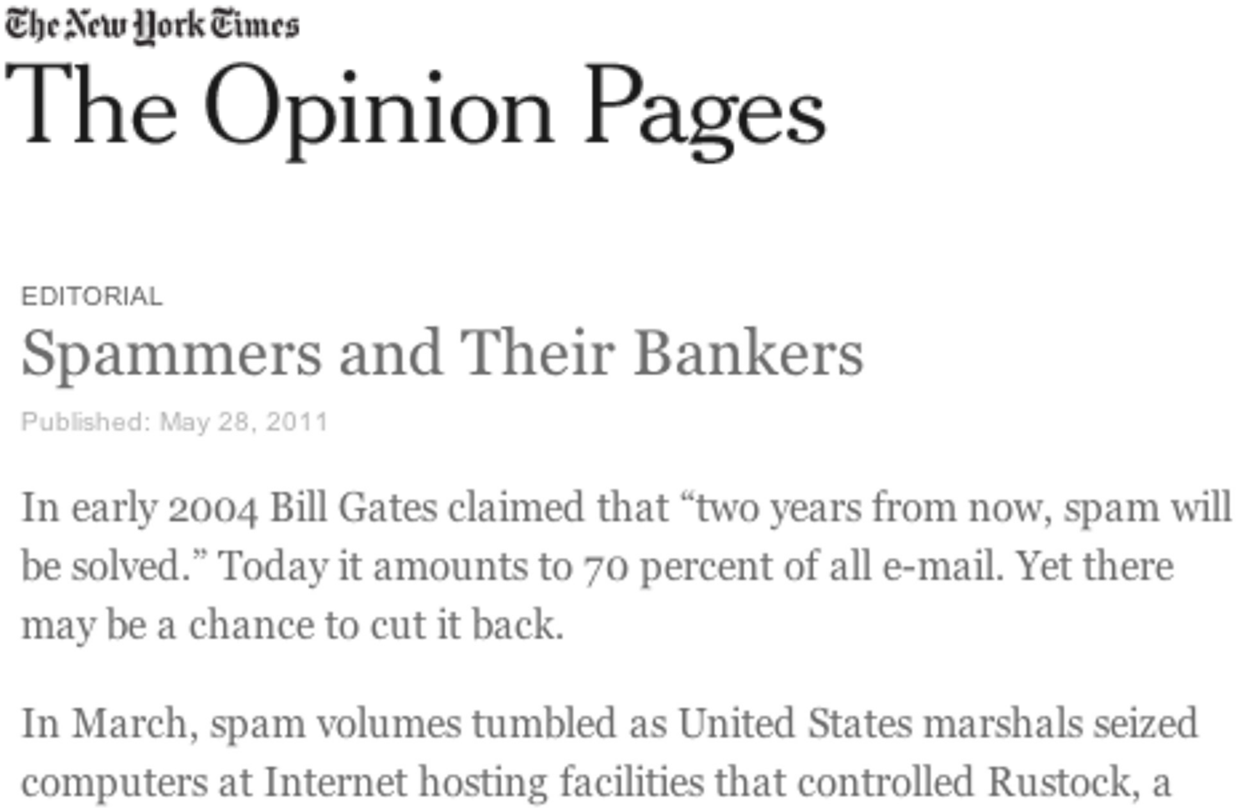


BINGO:
3 banks hosted
95+% of all sales

Results / Recommendations: Payment Interventions

- **Takedown**: action from “acquiring” (merchant) bank
  - Pressure to drop customers
  - Challenges: bi-lateral process, potentially slow

- **Blacklist**: action from “issuing” (consumer) banks
  - Few banks issue majority of US Visa/MC
  - Could demonetize spam ecosystem by refusing certain transactions with “bad” acquirers; fast
  - Challenges: incentives not aligned



The New York Times

The Opinion Pages

EDITORIAL

Spammers and Their Bankers

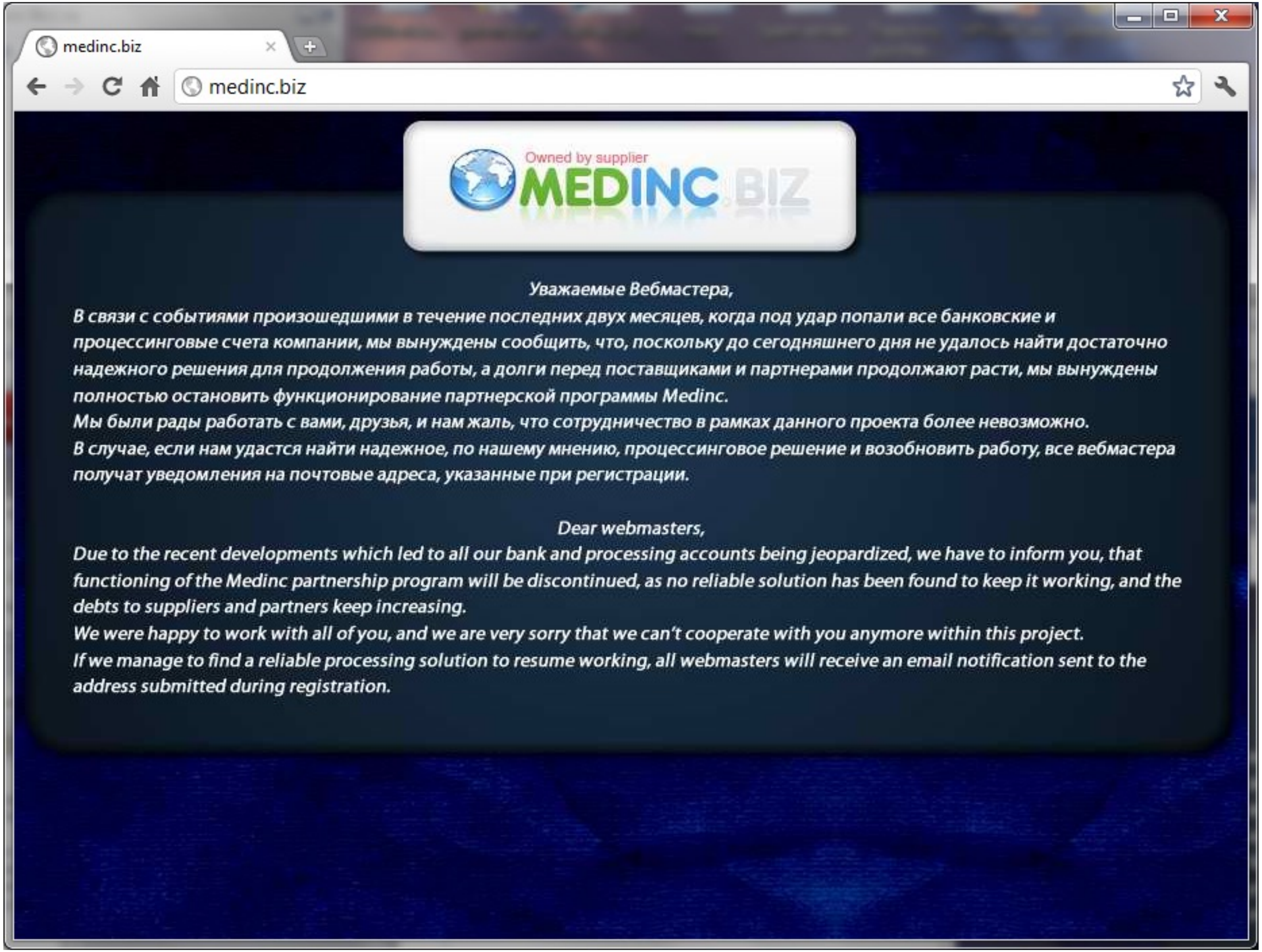
Published: May 28, 2011

In early 2004 Bill Gates claimed that “two years from now, spam will be solved.” Today it amounts to 70 percent of all e-mail. Yet there may be a chance to cut it back.

In March, spam volumes tumbled as United States marshals seized computers at Internet hosting facilities that controlled Rustock, a

The good news is there may be other ways to disrupt spammers. The Times’s John Markoff reported that computer scientists at two University of California campuses have found another vulnerability: spammers’ banks.

To track the flow of information, the researchers made hundreds of purchases. Buying Viagra from the Pharmacy Express group in Russia involved computers in Brazil, China and Turkey. The Viagra came from India. But 95 percent of the purchases were handled by three banks — in Azerbaijan, Latvia and St. Kitts and Nevis. This suggests that if banks



Уважаемые Вебмастера,

В связи с событиями произошедшими в течение последних двух месяцев, когда под удар попали все банковские и процессинговые счета компании, мы вынуждены сообщить, что, поскольку до сегодняшнего дня не удалось найти достаточно надежного решения для продолжения работы, а долги перед поставщиками и партнерами продолжают расти, мы вынуждены полностью остановить функционирование партнерской программы Medinc.

Мы были рады работать с вами, друзья, и нам жаль, что сотрудничество в рамках данного проекта более невозможно.

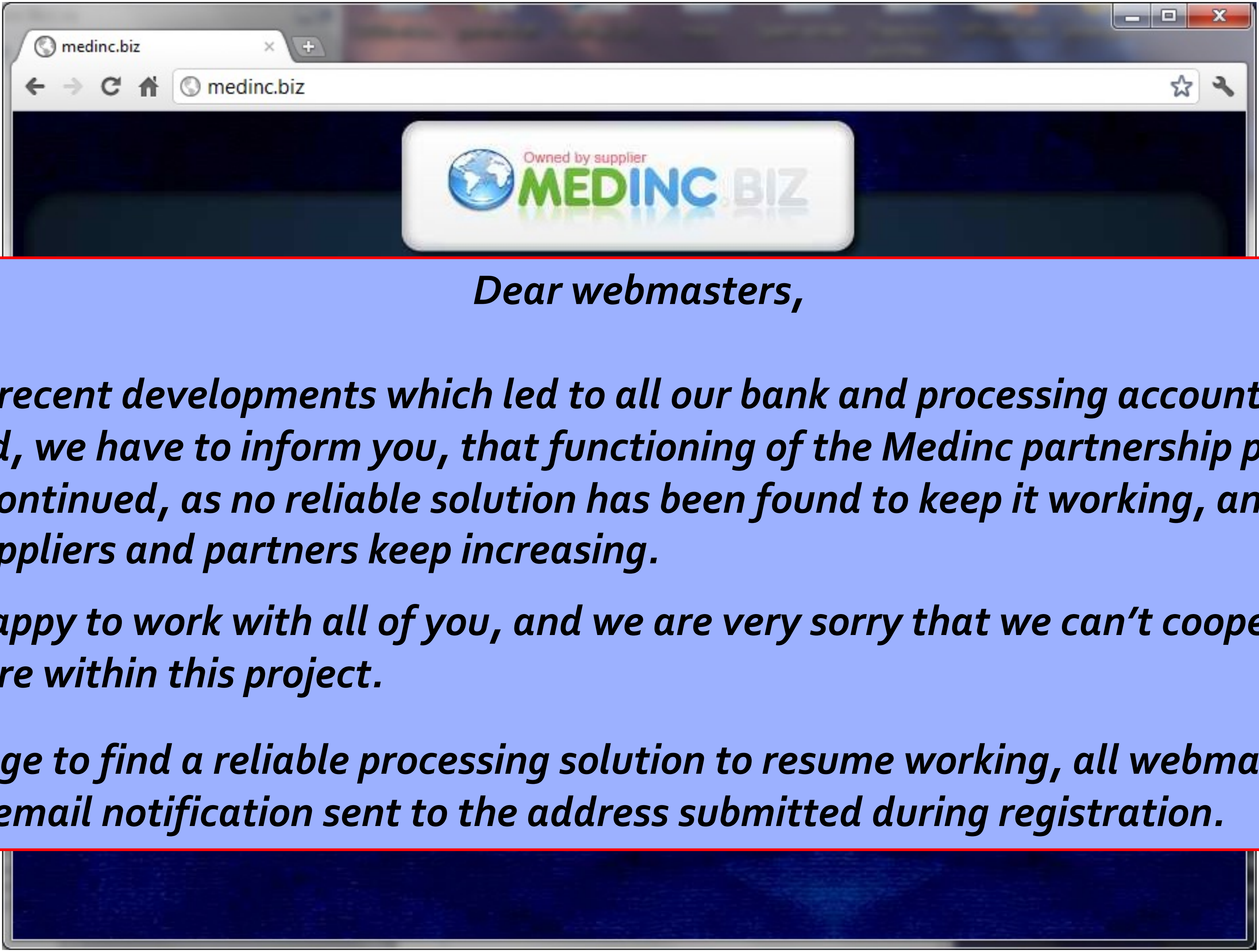
В случае, если нам удастся найти надежное, по нашему мнению, процессинговое решение и возобновить работу, все вебмастера получат уведомления на почтовые адреса, указанные при регистрации.

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.

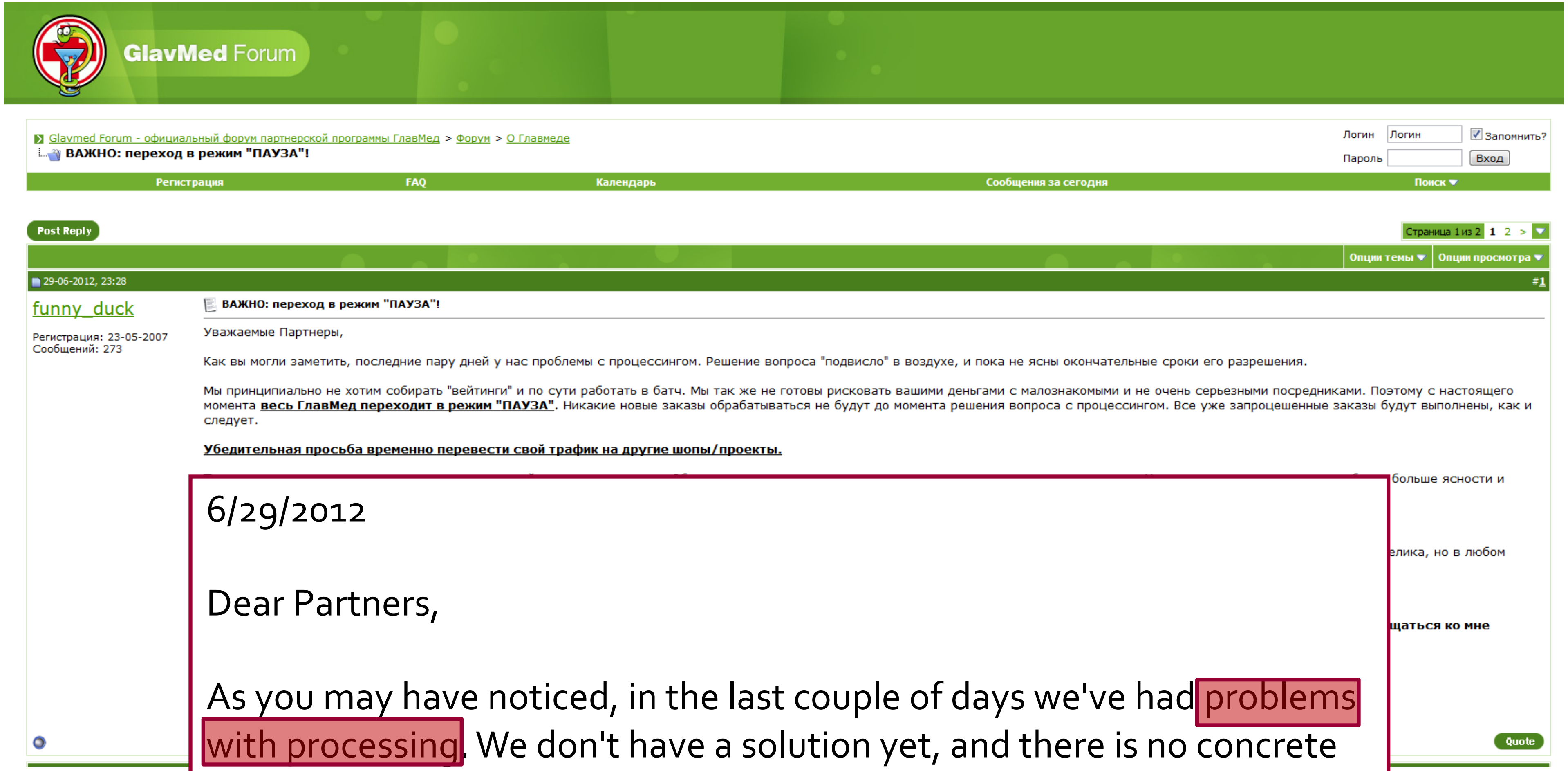


Dear webmasters,

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.



Glavmed Forum - официальный форум партнерской программы ГлавМед > Форум > О Главмеде

ВАЖНО: переход в режим "ПАУЗА"!

29-06-2012, 23:28

funny_duck

Регистрация: 23-05-2007
Сообщений: 273

ВАЖНО: переход в режим "ПАУЗА"!

Уважаемые Партнеры,

Как вы могли заметить, последние пару дней у нас проблемы с процессингом. Решение вопроса "подвисло" в воздухе, и пока не ясны окончательные сроки его разрешения.

Мы принципиально не хотим собирать "вейтинги" и по сути работать в батч. Мы так же не готовы рисковать вашими деньгами с малознакомыми и не очень серьезными посредниками. Поэтому с настоящего момента **весь ГлавМед переходит в режим "ПАУЗА"**. Никакие новые заказы обрабатываться не будут до момента решения вопроса с процессингом. Все уже запроцешенные заказы будут выполнены, как и следует.

Убедительная просьба временно перевести свой трафик на другие шопы/проекты.

больше ясности и

елика, но в любом

щаться ко мне

6/29/2012

Dear Partners,

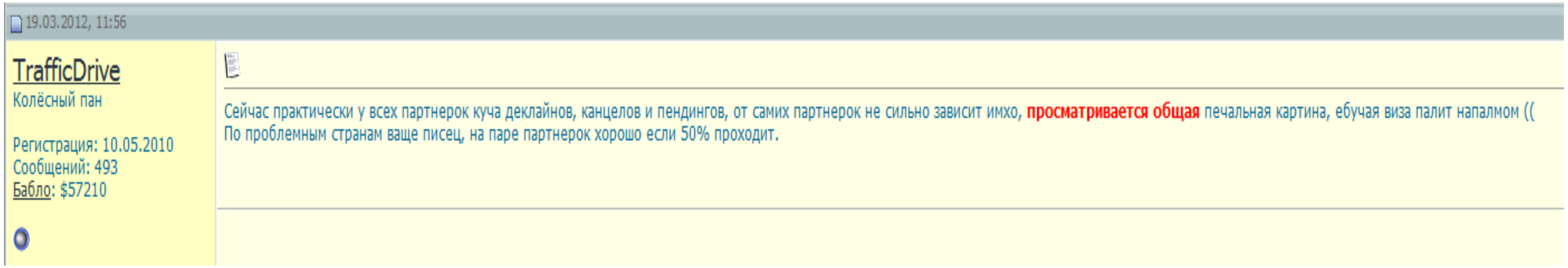
As you may have noticed, in the last couple of days we've had problems with processing. We don't have a solution yet, and there is no concrete time when it will be resolved.

....

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.

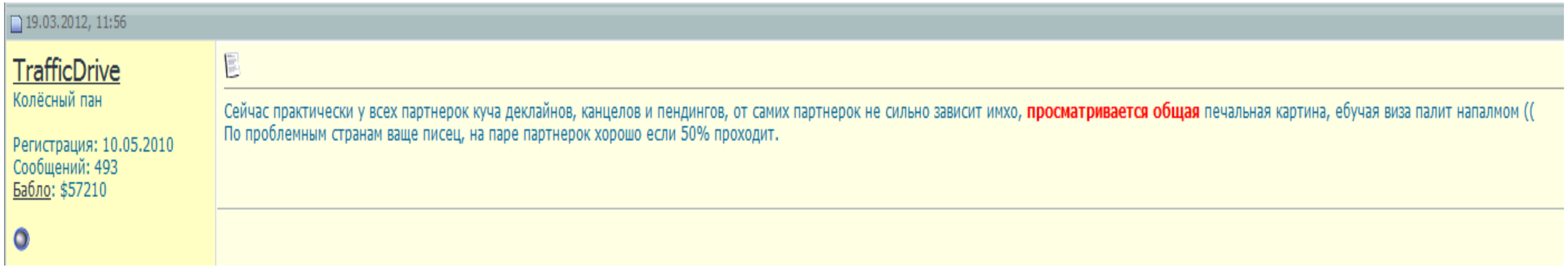


19.03.2012, 11:56

TrafficDrive
Колёсный пан

Регистрация: 10.05.2010
Сообщений: 493
Бабло: $57210

Сейчас практически у всех партнерок куча деклайнов, канцелов и пендингов, от самих партнерок не сильно зависит имхо, **просматривается общая** печальная картина, ебучая виза палит напалмом ((
По проблемным странам ваще писец, на паре партнерок хорошо если 50% проходит.



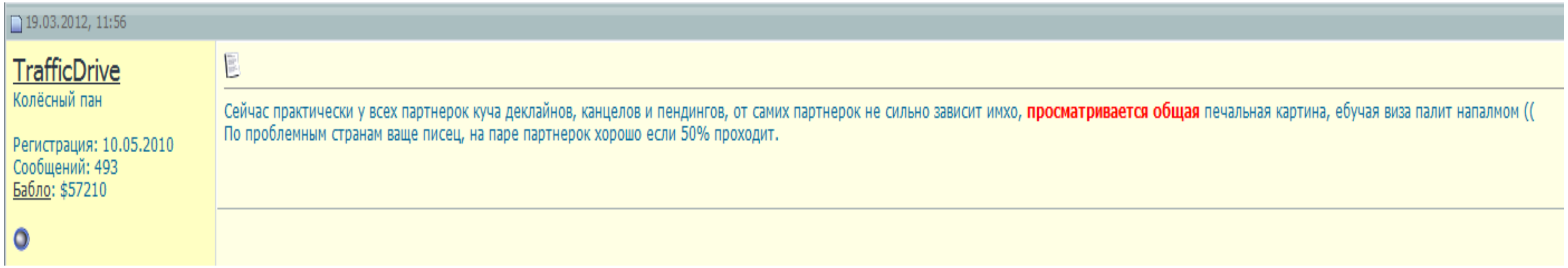
19.03.2012, 11:56

TrafficDrive
Колёсный пан

Регистрация: 10.05.2010
Сообщений: 493
Бабло: $57210

Сейчас практически у всех партнерок куча деклайнов, канцелов и пендингов, от самих партнерок не сильно зависит имхо, **просматривается общая** печальная картина, ебучая виза палит напалмом ((
По проблемным странам ваще писец, на паре партнерок хорошо если 50% проходит.

"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)."



19.03.2012, 11:56

TrafficDrive
Колёсный пан

Регистрация: 10.05.2010
Сообщений: 493
Бабло: $57210

Сейчас практически у всех партнерок куча деклайнов, канцелов и пендингов, от самих партнерок не сильно зависит имхо, **просматривается общая** печальная картина, ебучая виза палит напалмом ((
По проблемным странам ваще писец, на паре партнерок хорошо если 50% проходит.

"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)."

Discussion

Ethics

- Conducting this research (e.g., purchasing spam merchandise)?
- Ethics of spam & whether it constitutes abuse/attacks?

Relevance & Utility of Analysis Today

- What kinds of problems would this analysis be useful for today, and how would the research get conducted?
- What challenges might this analysis face today?

Next Class

- Read & Respond to Denial of Services Papers

- Paper Presenter & Discussion Lead Signups:
  - Sent out list of papers for presenting on Canvas
  - Sign-ups next class
  - Initial two weeks: papers can be presented by pairs of students (afterward, just one student per paper)
  - Slides for presentation due at 11:00am before class; no written responses due from you for that class.
  - Reach out if you want feedback / have confusion about paper