Empiricism

vs.

The Underground Economy

Christian Kreibich

K. Levchenko, C. Kanich, C. Grier, A. Pitsillidis,

B. Enright, N. Cachra, M. Felegyhazi, T. Halvorson, H. Liu,

D. McCoy, N. Weaver, V. Paxson, G.M. Voelker, S. Savage

International Computer Science Institute

UC San Diego

The International Computer Science Institute

- Independent, non-profit research lab
- Affiliated with UC Berkeley
- Mission: basic computer science
- 6 groups: AI, multimedia, networking, research initiatives, speech, vision
- Networking group: measurement, security, architecture

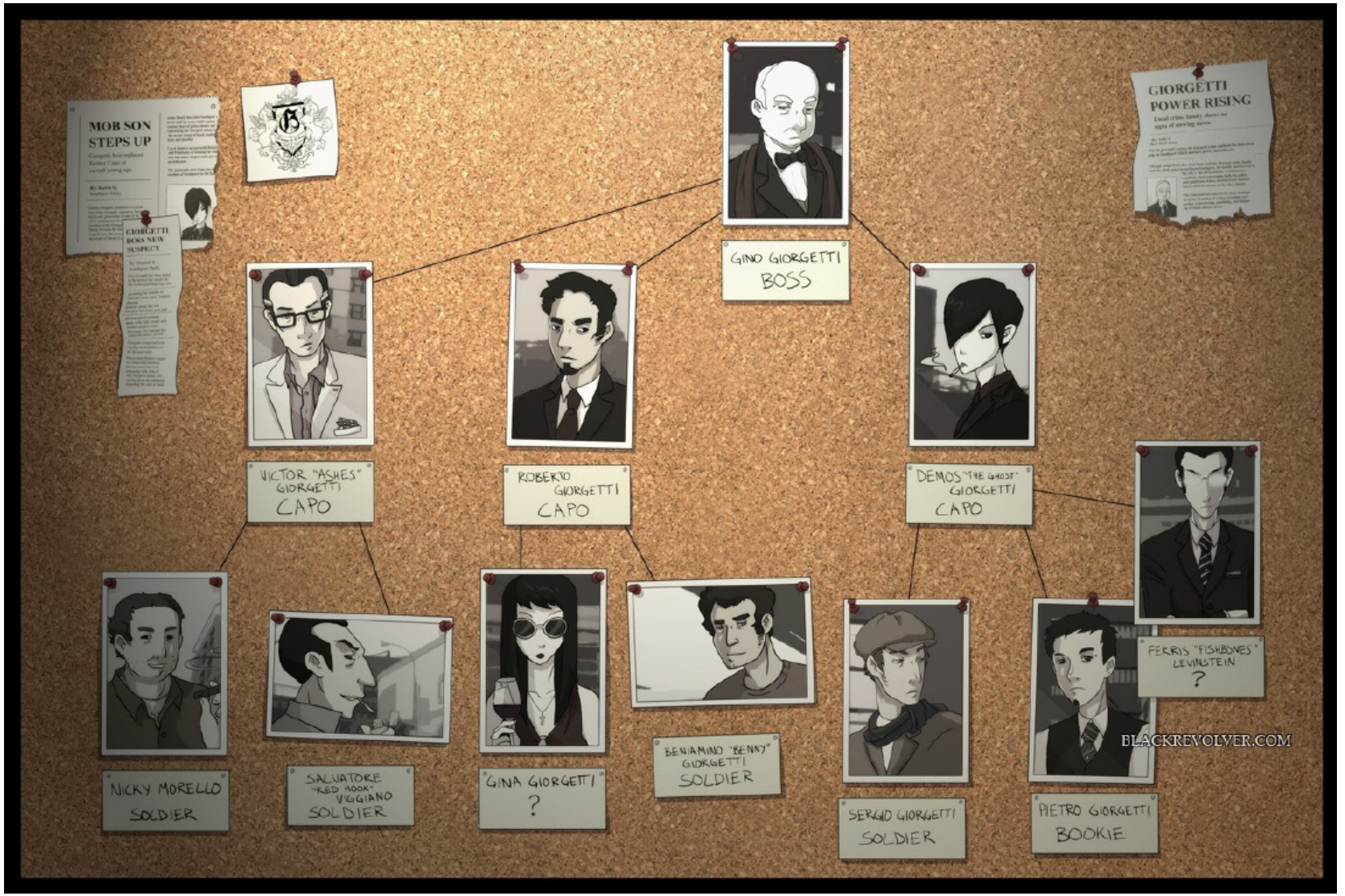
OMFG!

2008

ROBOT

ZOMBIE

n Bot·net


MOB SON STEPS UP
GIORGETTI BOSS NEW SUSPECT
GIORGETTI POWER RISING
GINO GIORGETTI
BOSS
VICTOR "ASHES" GIORGETTI
CAPO
ROBERTO GIORGETTI
CAPO
DEMOS "THE GHOST" GIORGETTI
CAPO
NICKY MORELLO
SOLDIER
SALVATORE "RED HOOK" VIGGIANO
SOLDIER
GINA GIORGETTI
?
BENIAMINO "BENNY" GIORGETTI
SOLDIER
SERGIO GIORGETTI
SOLDIER
PIETRO GIORGETTI
BOOKIE
FERRIS "FISHBONES" LEVINSTEIN
?
BLACKREVOLVER.COM

n Bot·net

n Bot·net

Storm worm 'making millions a day'

Compromised machines sending out highly profitable spam, says IBM security strategist

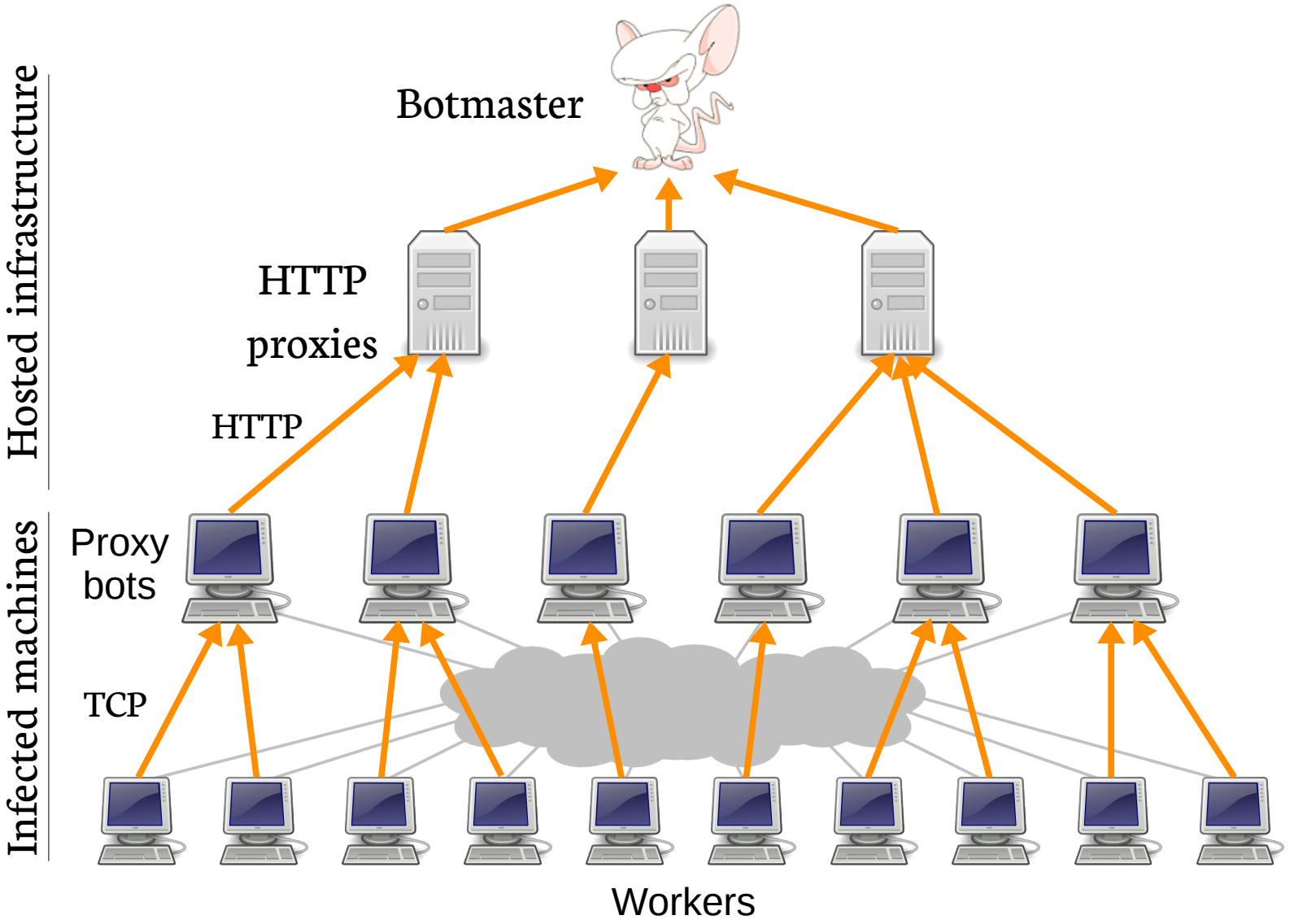
Clive Akass, Personal Computer World 11 Feb 2008

The people behind the Storm worm are making millions of pounds a day by using it to generate revenue, according to IBM's principal web security strategist.

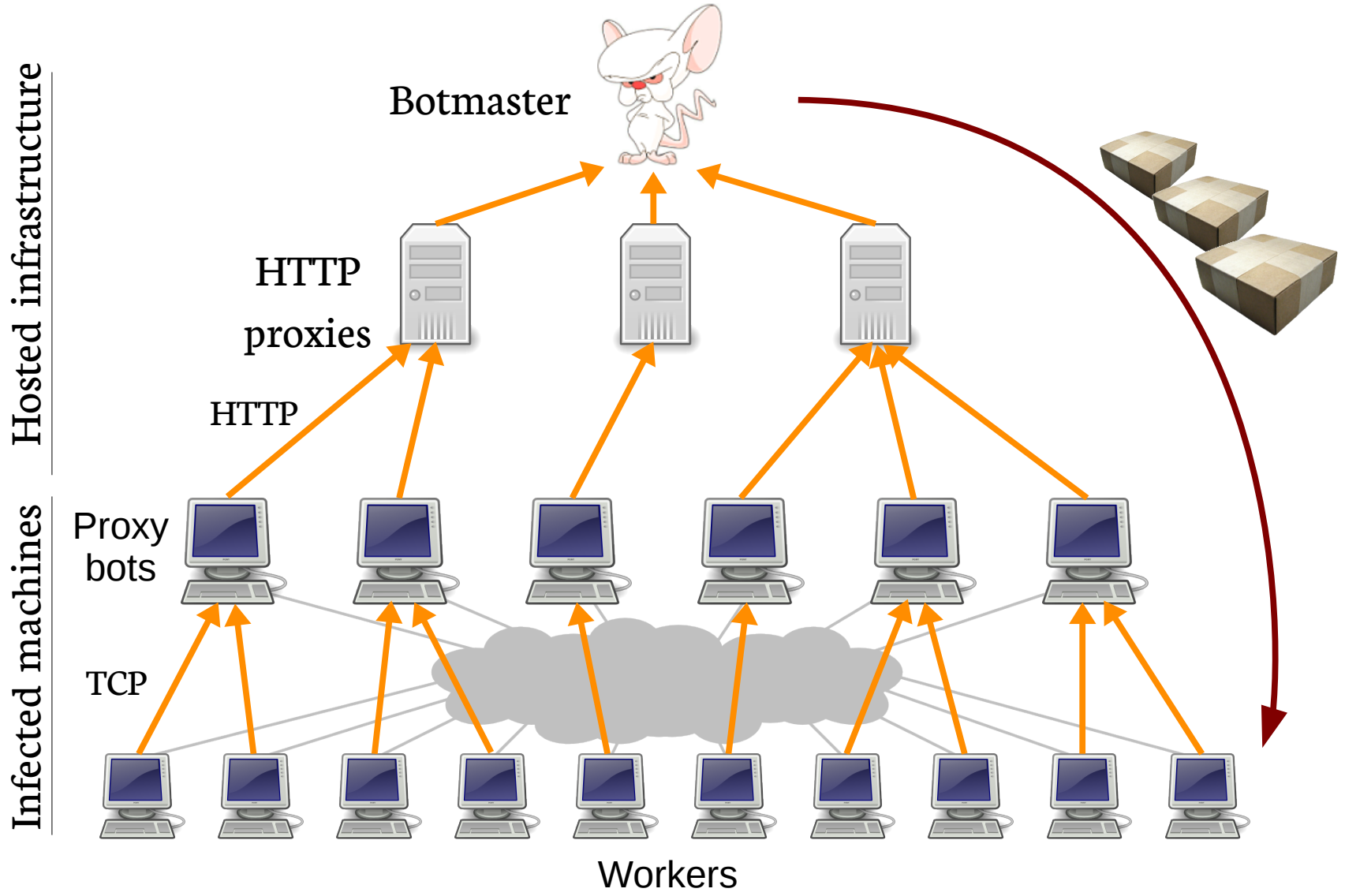
Joshua Corman, of **IBM Internet Security Systems**, said that in the past it had been assumed that web security attacks were essential ego driven.

Part I
Spam conversion rates

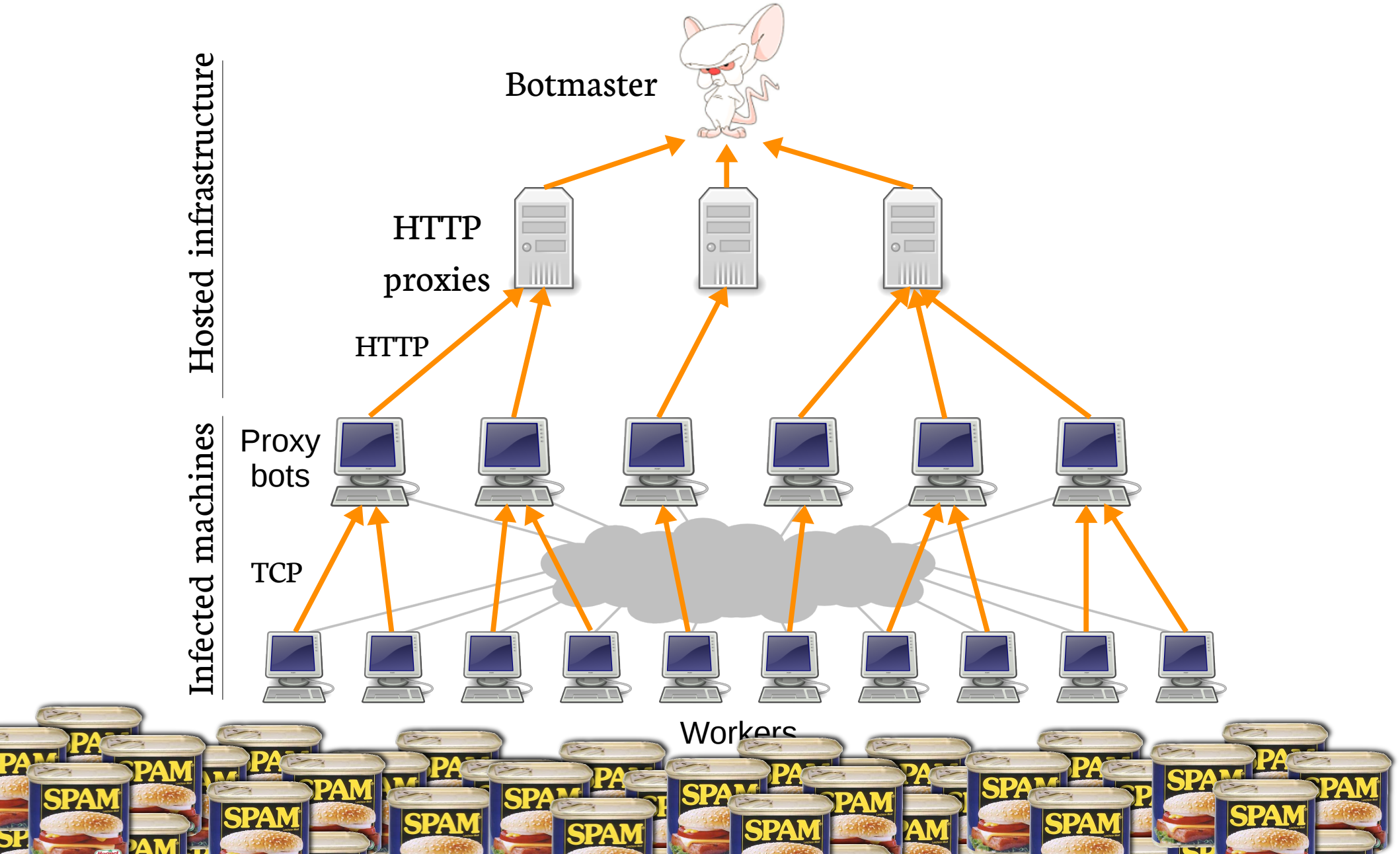
The Storm botnet



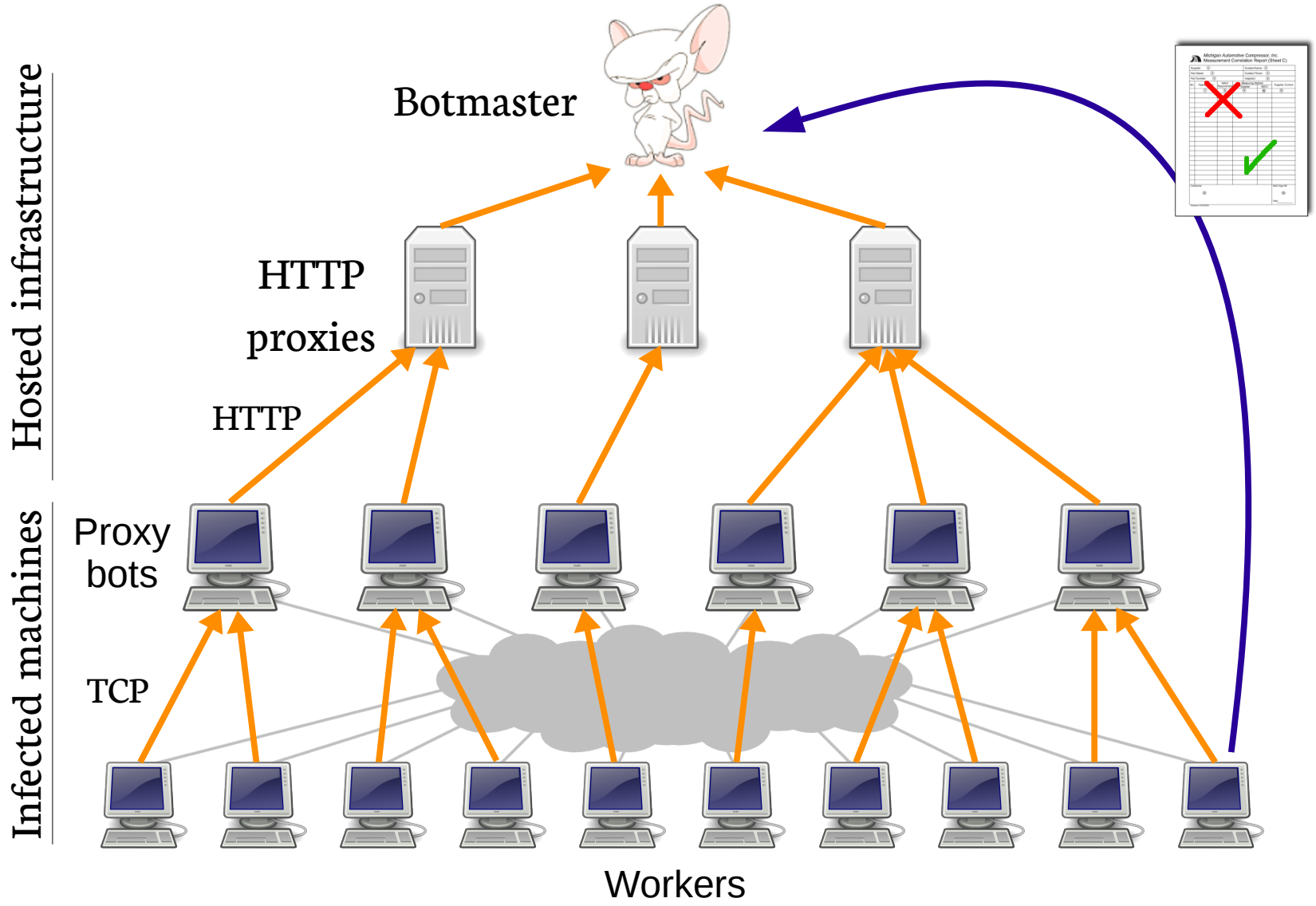
Spamming procedure



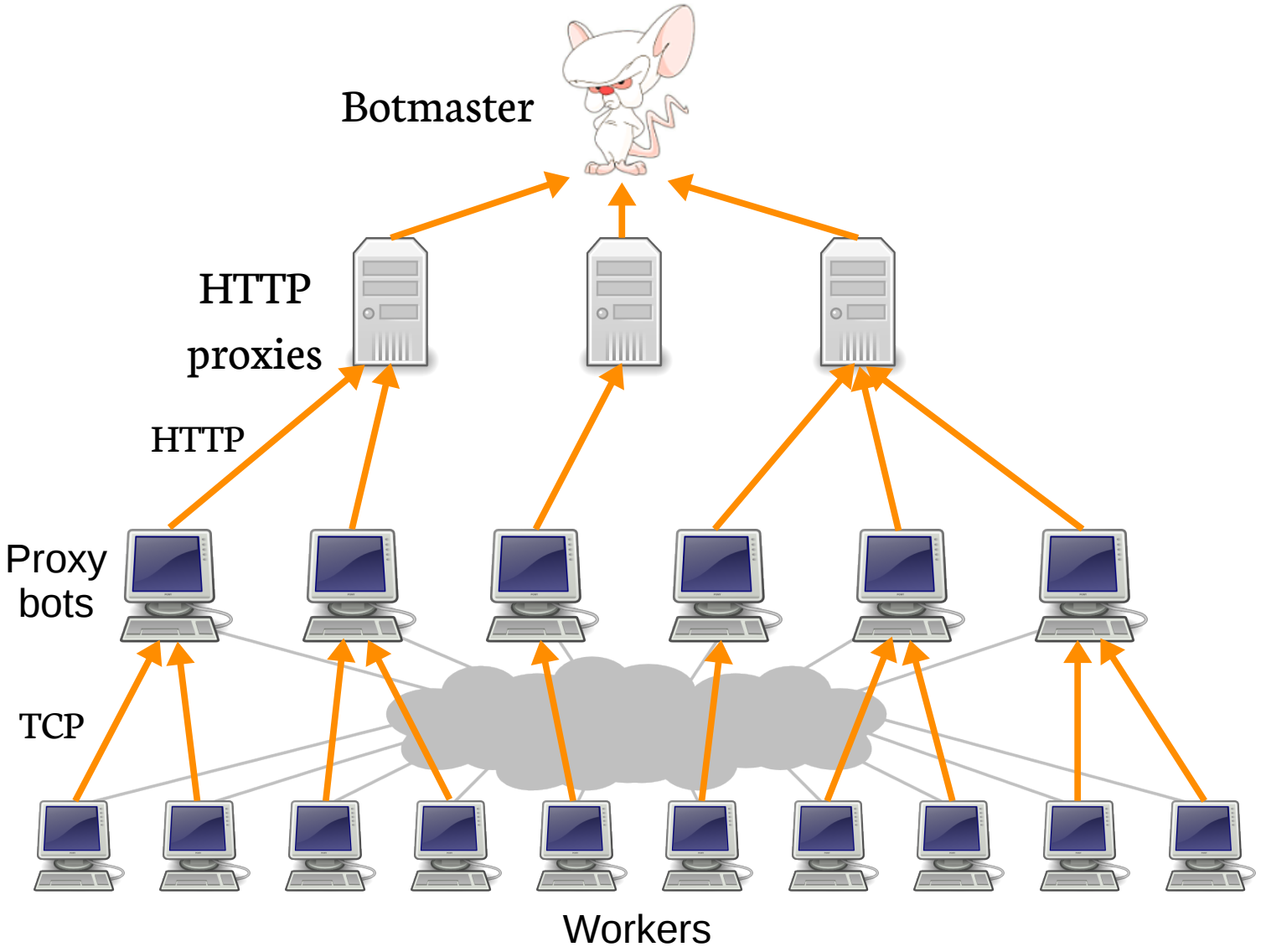
Spamming procedure



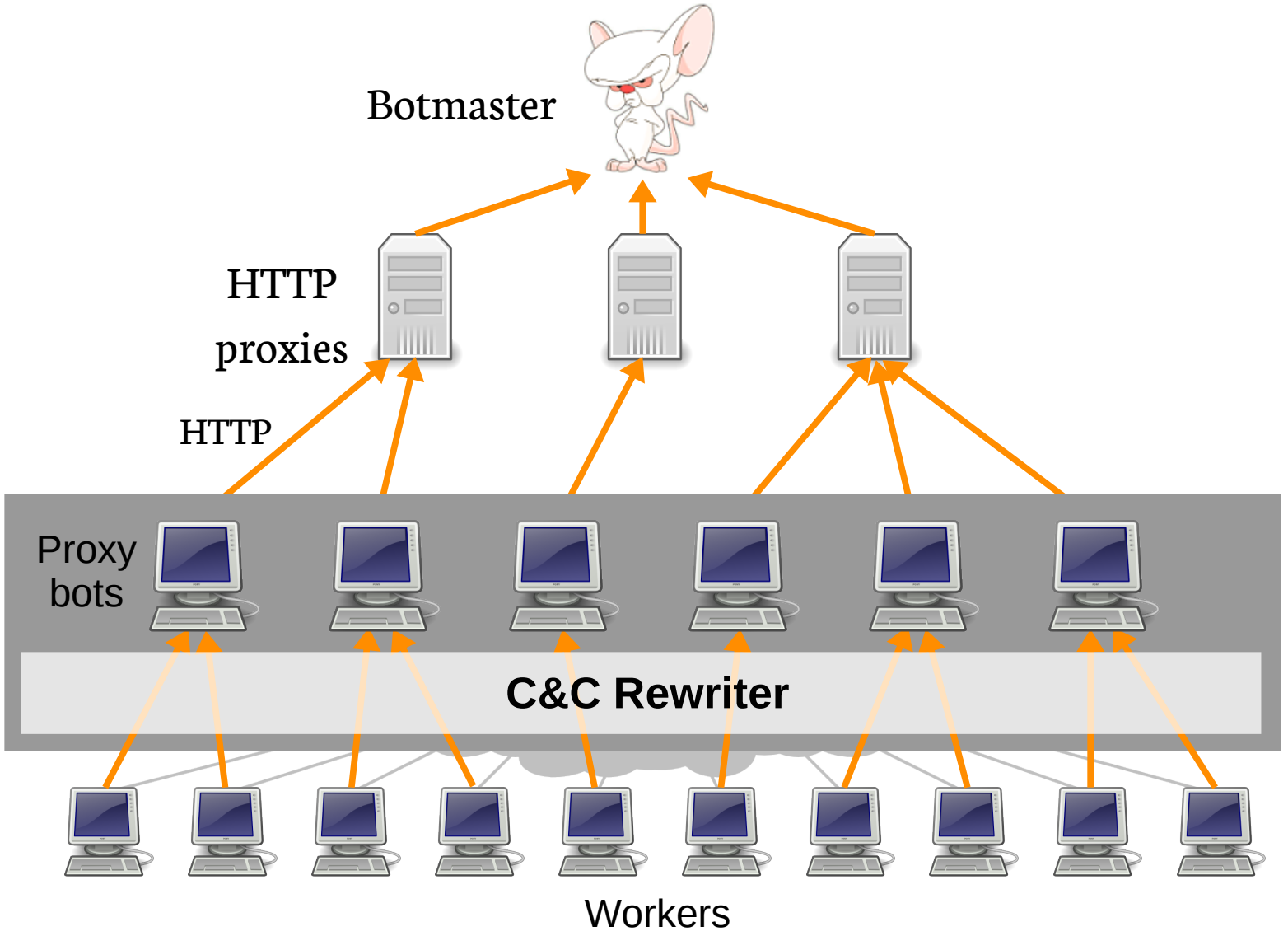
Spamming procedure



Wait a minute, no crypto!



We can … change instructions.



Idea

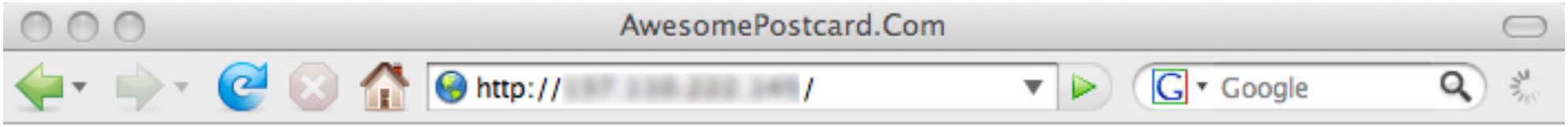
- Infiltrate middle tier of botnet
- Rewrite existing spamming instructions
- Send customers to our own servers
- Measure traffic along the way

Received: (qmail 3871 invoked from network); Tue, 15 Jan 2008
08:26:26
Received: from unknown (HELO gug) (211.219.143.28)
        by ukdewkg with SMTP; Tue, 15 Jan 2008 08:26:26 -0800
Message-ID: <478CDEB2.4000300@ot2sen.dk>
Date: Tue, 15 Jan 2008 08:26:26 -0800
From: <slbc@ot2sen.dk>
User-Agent: Thunderbird 2.0.0.6 (Windows/20070728)
MIME-Version: 1.0
To: davidtyler@aureate.com
Subject: Results proved by thousands of men!
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

Trustworthy way to fight failures!
http://canadianpharmacyproducts.com

```
Received: (qmail 3871 invoked from network); Tue, 15 Jan 2008
08:26:26
Received: from unknown (HELO gug) (211.219.143.28)
          by ukdewkg with SMTP; Tue, 15 Jan 2008 08:26:26 -0800
Message-ID: <478CDEB2.4000300@ot2sen.dk>
Date: Tue, 15 Jan 2008 08:26:26 -0800
From: <slbc@ot2sen.dk>
User-Agent: Thunderbird 2.0.0.6 (Windows/20070728)
MIME-Version: 1.0
To: davidtyler@aureate.com
Subject: Results proved by thousands of men!
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

Trustworthy way to fight failures!
http://murmuraverse.com/prod=gdylgwbohuCdxuhdwh1frp
```



Your download will start in 5 seconds.
If your download does not start, click here

Canadian Pharmacy

http://[redacted]/

Google

Home | Bestsellers | All products | FAQ | Contact us

$ € £

Pharma Bonus

Your cart: **$0.00** (0 items)
Proceed to Checkout ›

Canadian Pharmacy
#1 Internet Online Drugstore

Products list

- **Bestsellers**
- Male Enhancement
- Men's Health
- SALES - 20% OFF
- Female Enhancement
- Weight Loss
- Gums New!
- Body-Building
- Hypnotherapy

Viagra + Cialis 69.99$

10 x Viagra
100 mg
10 x Cialis
20 mg

ORDER NOW

Growth Pack 179.95$

Growth Pills
1 bottle x 60caps
Growth Oil
1 tube x 2oz

ORDER NOW

Viagra 225.61$

120 pills
100 mg
+4 Free pills

ORDER NOW

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 5

Search:

Today's Bestsellers

Viagra

Our price
$1.21

More info | Add to cart

Cialis

Our price
$2.18

More info | Add to cart

Viagra Professional

Our price
$3.73

More info | Add to cart

Done

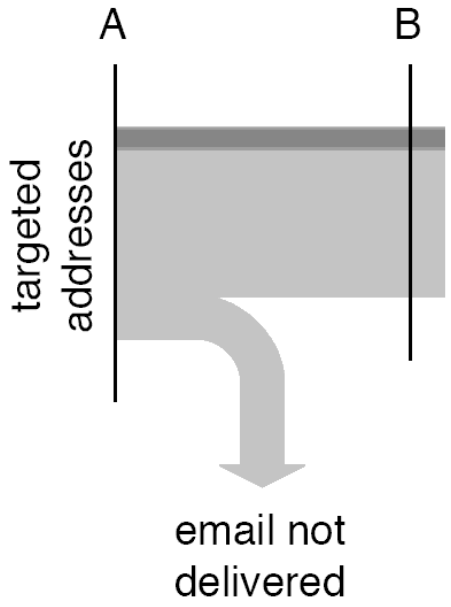
Campaign volumes

Campaign	Dates	Workers	E-mails
Pharmacy	Mar 21 – Apr 15	31,348	347,590,389
Postcard	Mar 9 – Mar 15	17,639	83,665,479
April Fool	Mar 31 – Apr 2	3,678	38,651,124
		Total	469,906,992

Conversion rates

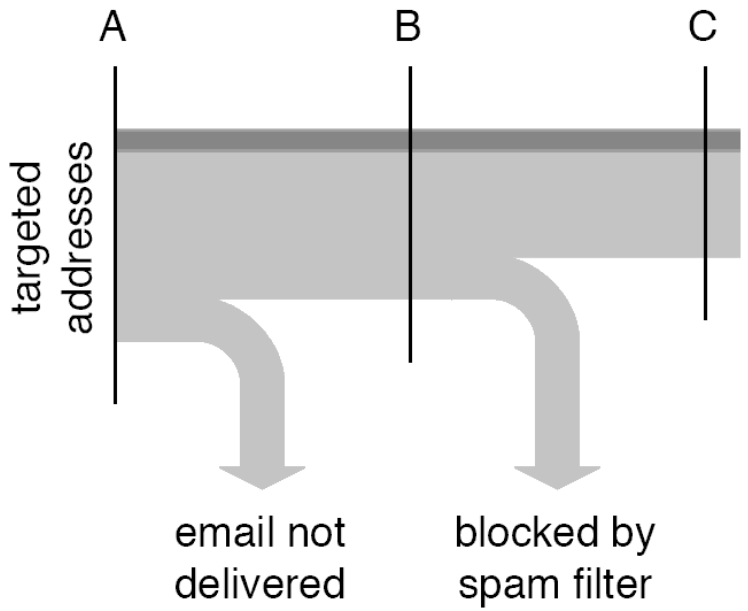
Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%

Conversion rates



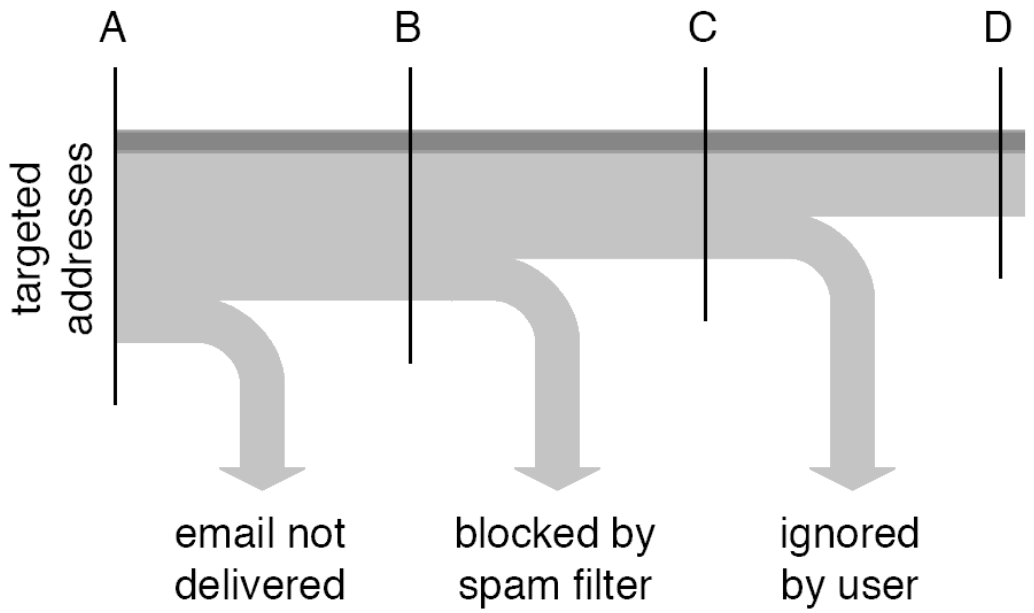
Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%
B – MTA Delivery (est.)	82,700,000	23.8%	21,100,000	25.2%	10,100,000	25.2%

Conversion rates



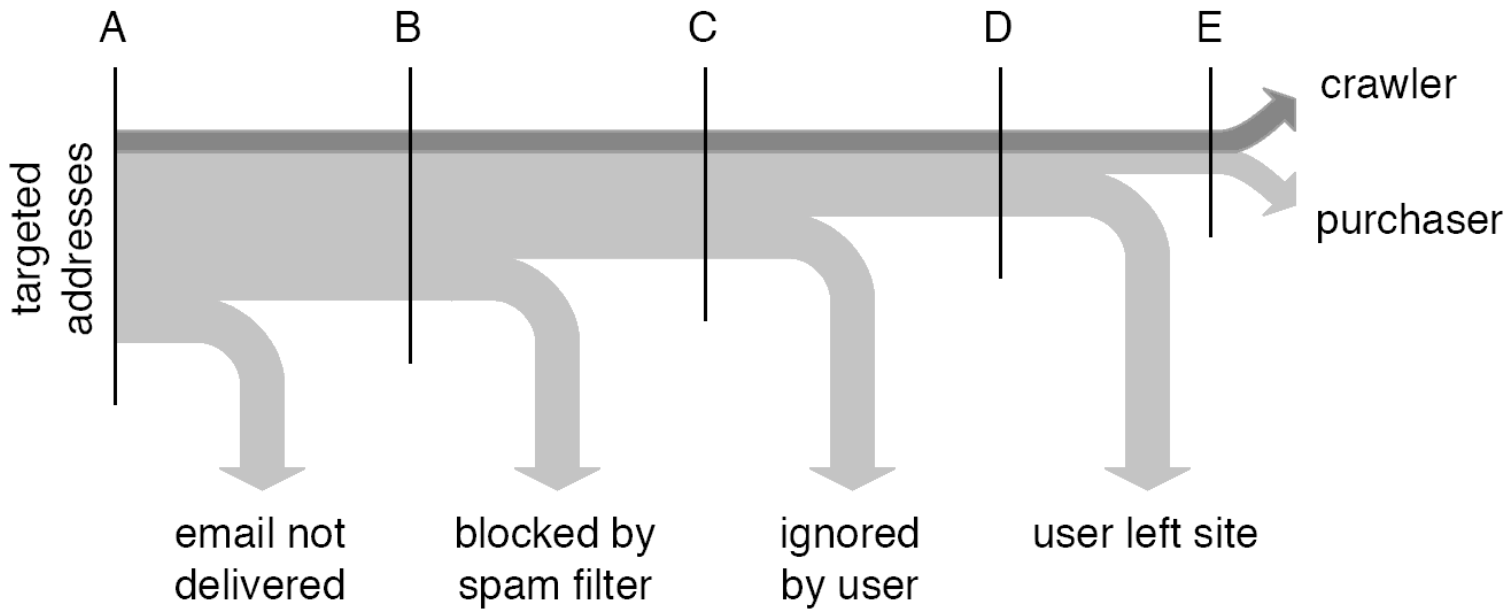
Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%
B – MTA Delivery (est.)	82,700,000	23.8%	21,100,000	25.2%	10,100,000	25.2%
C – Inbox Delivery	—	—	—	—	—	—

Conversion rates



Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%
B – MTA Delivery (est.)	82,700,000	23.8%	21,100,000	25.2%	10,100,000	25.2%
C – Inbox Delivery	—	—	—	—	—	—
D – User Site Visits	10,522	0.00303%	3,827	0.00457%	2,721	0.00680%

Conversion rates



Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%
B – MTA Delivery (est.)	82,700,000	23.8%	21,100,000	25.2%	10,100,000	25.2%
C – Inbox Delivery	—	—	—	—	—	—
D – User Site Visits	10,522	0.00303%	3,827	0.00457%	2,721	0.00680%
E – User Conversions	28	0.0000081%	316	0.000378%	225	0.000561%

1 in 12.5M

1 in 265K

1 in 178K

1 in 10

Pharmaceutical revenues

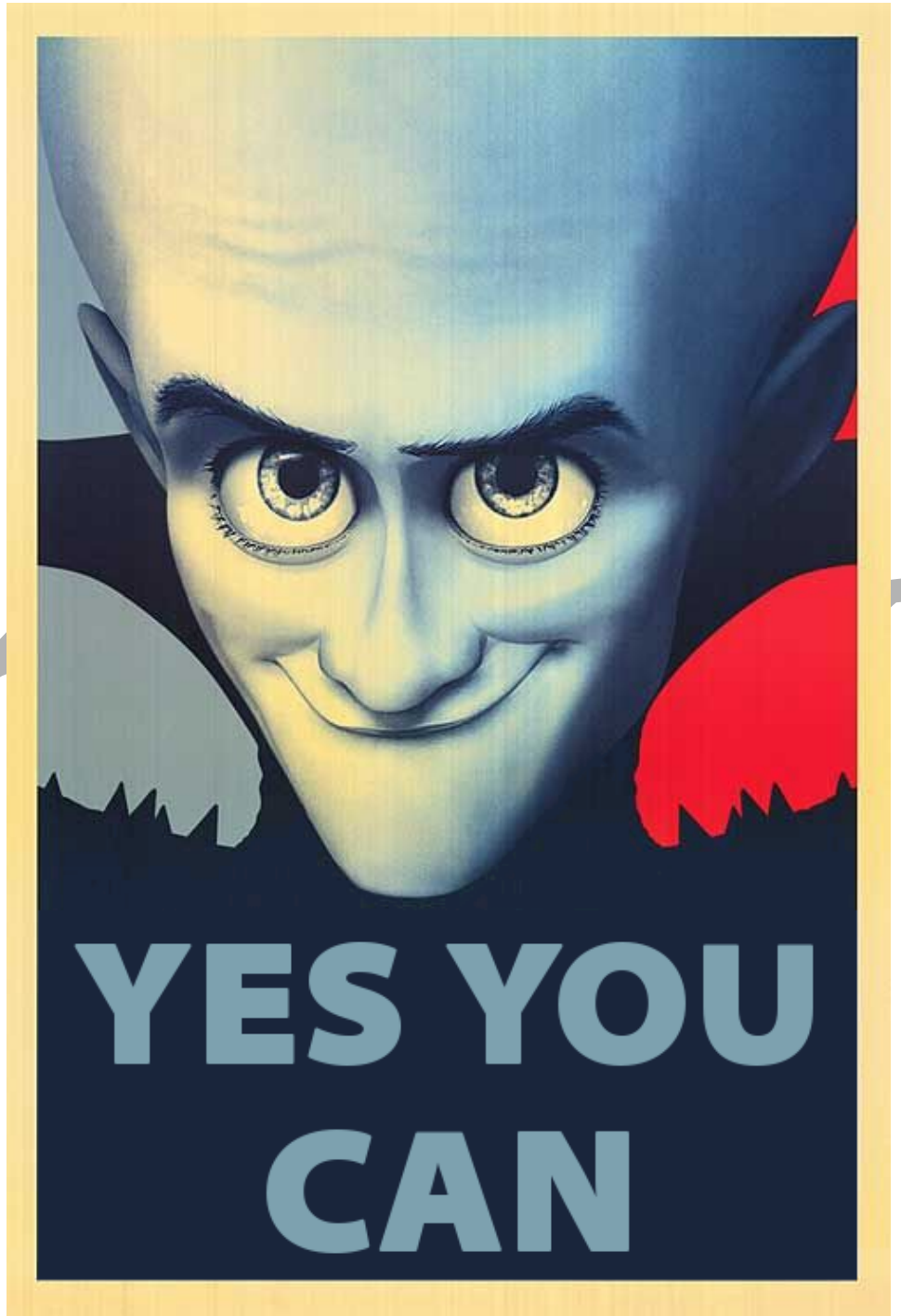
- 28 purchases in 26 days, average price ~$100
  - Total: $2,732, $140/day
- But: we interposed only on ~1.5% of workers!
  - $9500/day (and 8500 bots per day)
  - $3.5M/year
- Storm: service provider or integrated setup?
  - Retail price of spam ~$80 per million
  - Suggests integrated operation to be profitable
  - In fact: 40% commission for botmasters via affiliate program

Part II
Click trajectories

MHMM...

I WANT $$$ TOO!

I w TOO!



I W TOO!

Добро пожаловать на RX-Promotion

RX-Promotion — партнерская программа, позволяющая участникам зарабатывать продаже медикаментов там, где они хотят и так, как они хотят. Можно открыть собственную онлайн-аптеку или работать через нашу сеть.

Главное — это найти покупателя и продать медикаменты. Ну и, конечно, не забыть получить прибыль: вплоть **до 60% от сделки**. Считаете это предложение невыгодным? Что ж, остается вам только позавидовать.

Кстати, а сейчас мы разыгрываем Золотой Слиток.

Тех.отдел

Общие вопросы
ICQ: 402961146
ICQ: 457098148

Тех. вопросы
ICQ: 50423090

Ещё ICQ

Skype:
rx-promotion

РЕГИСТРАЦИЯ

У нас отлично:

КОМИССИЯ ДО 60%
ПО РЕФЕРАЛАМ ДО 15%

30-50% Sale Comissions

On-demand Payments

Low Drug prices

Run your own shop

получить прибыль: вплоть **до 60% от сделки**. Считаете это предложение невыгодным? Что ж, остается вам только позавидовать.

Кстати, а сейчас мы разыгрываем Золотой Слиток.

rx-promotion

РЕГИСТРАЦИЯ

У нас отлично:

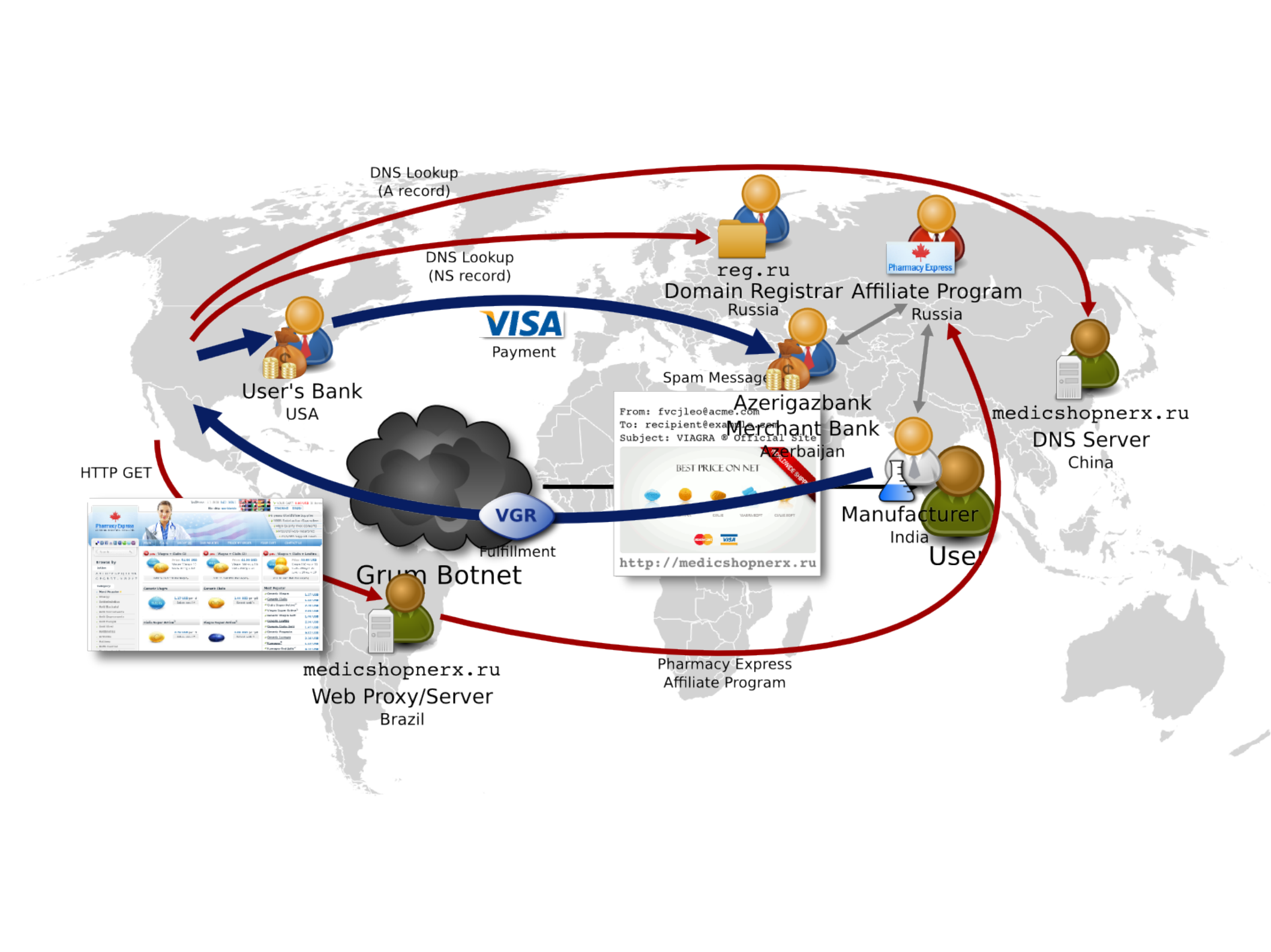
Detailed Stats

attractive customer Support

Contests!

Parties!

A purchase


DNS Lookup
(A record)
DNS Lookup
(NS record)
reg.ru
Domain Registrar
Russia
Affiliate Program
Russia
Pharmacy Express
VISA
Payment
User's Bank
USA
Spam Message
Azerigazbank
Merchant Bank
Azerbaijan
medicshopnerx.ru
DNS Server
China
From: fvcjleo@acme.com
To: recipient@example.com
Subject: VIAGRA ® official site
BEST PRICE ON NET
http://medicshopnerx.ru
HTTP GET
VGR
Fulfillment
Grum Botnet
Manufacturer
India
User
medicshopnerx.ru
Web Proxy/Server
Brazil
Pharmacy Express
Affiliate Program

Idea

- Map technical infrastructure
  - URL crawling
- Map financial infrastructure
  - Make purchases!
- Identify bottlenecks

1 Feed Collection

Spam Feeds

http://sdfjsdf.ru
http://pillsale.cn
drugz.com
http://capharma.com

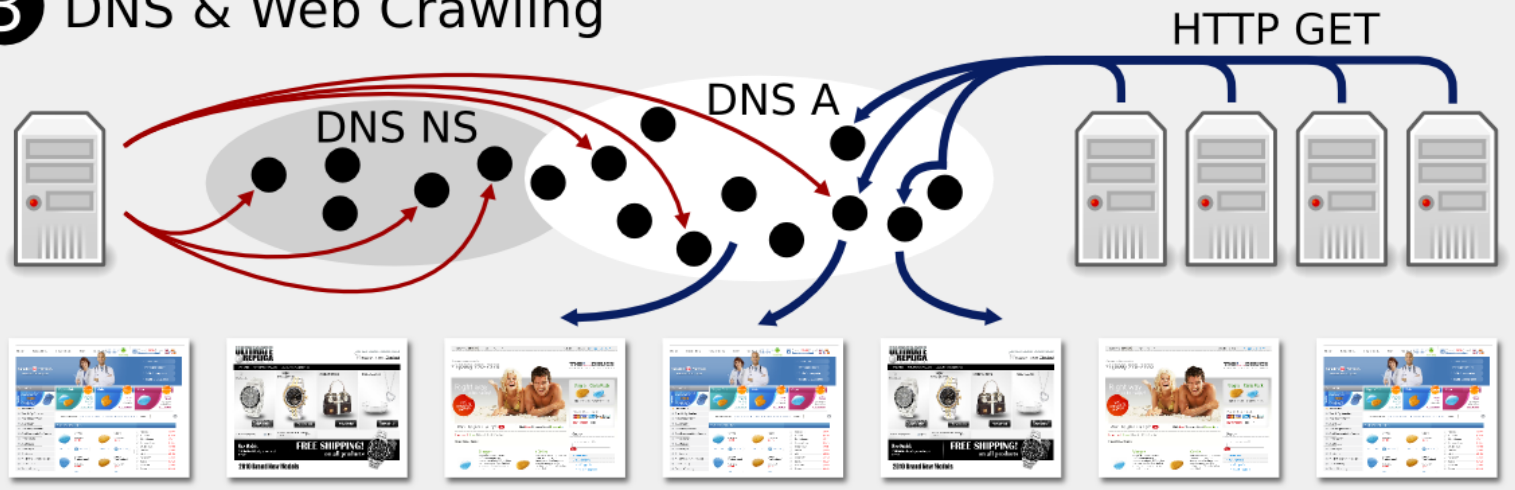
URL Feeds

Botfarm Spam Feed

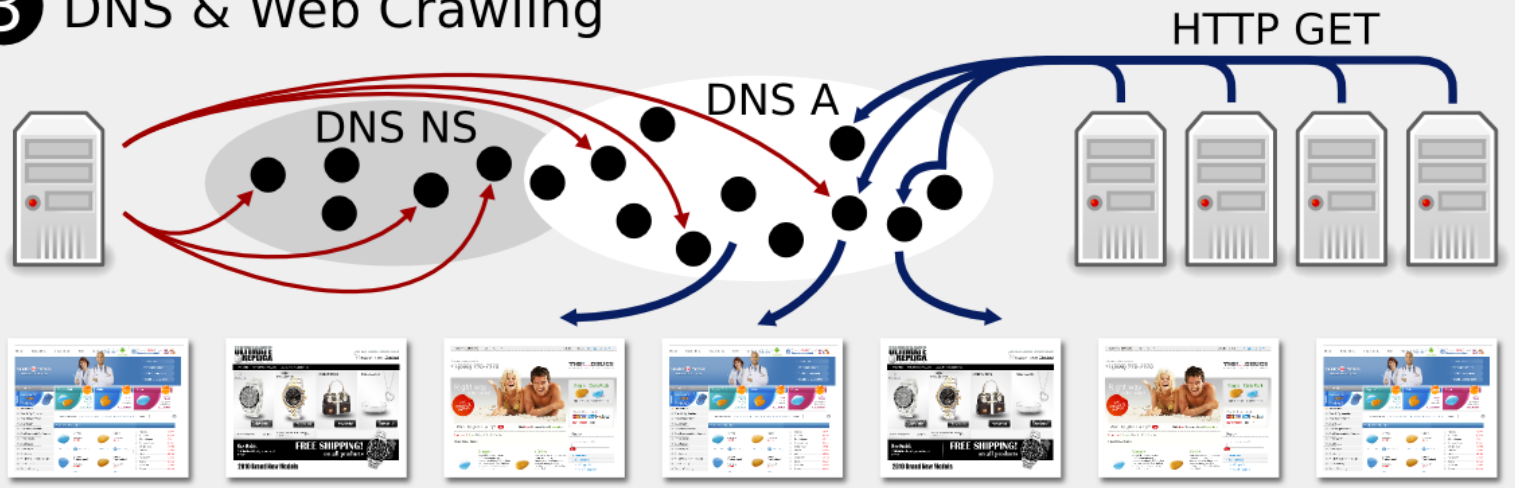
2 URL Extraction

http://cheapdrugz.com
http://pillsale.cn

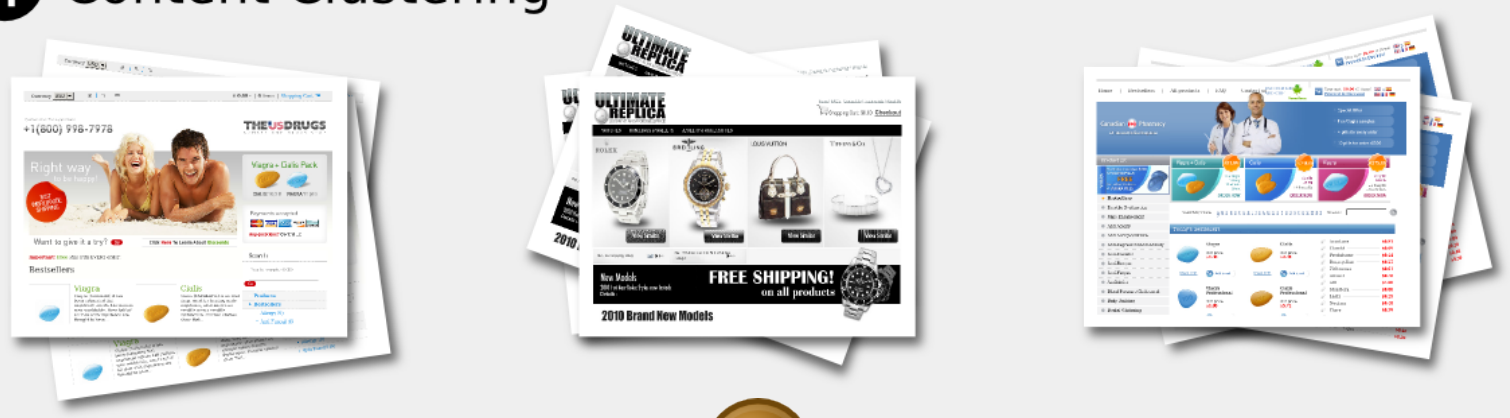
3 DNS & Web Crawling



3 DNS & Web Crawling



4 Content Clustering



5 Content Tagging

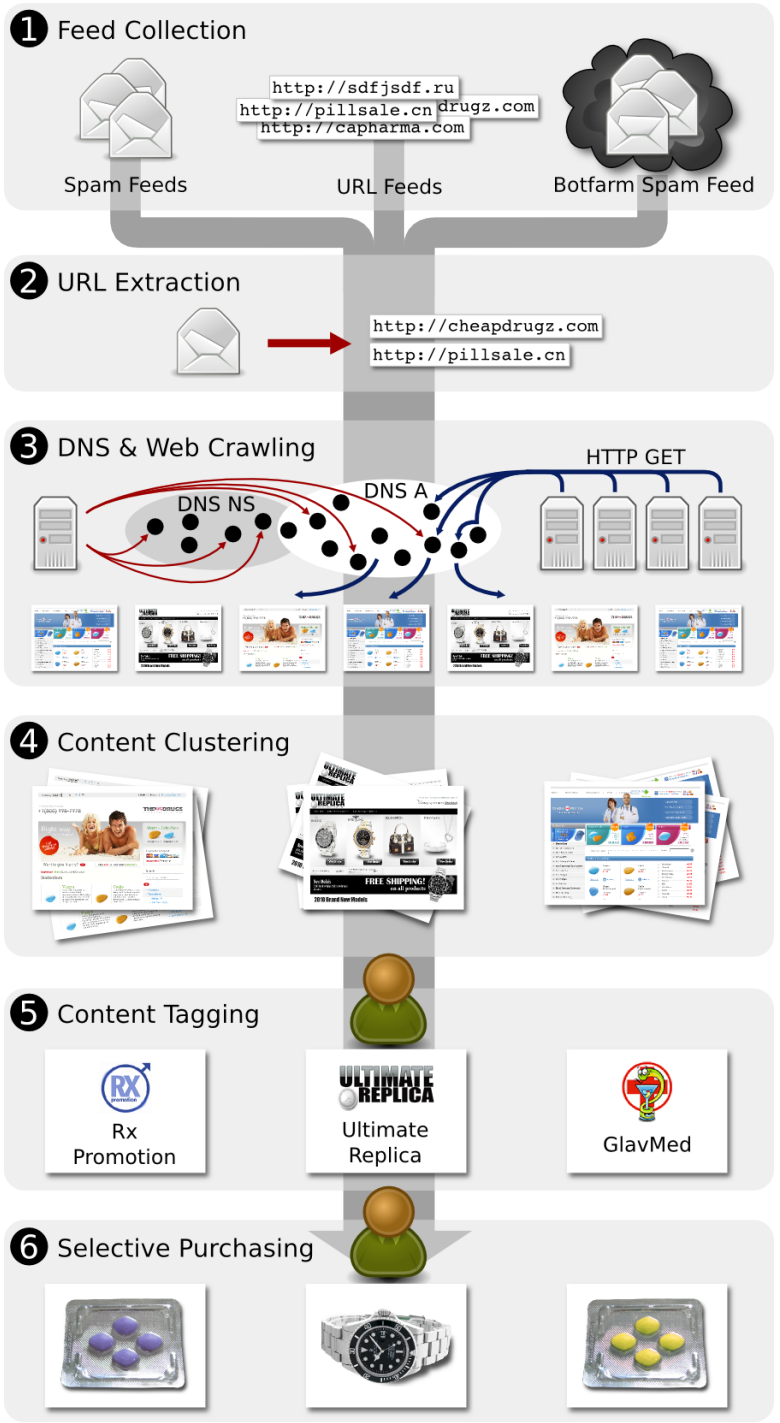
Rx Promotion	Ultimate Replica	GlavMed

4 Content Clustering

5 Content Tagging

Rx Promotion	Ultimate Replica	GlavMed

6 Selective Purchasing

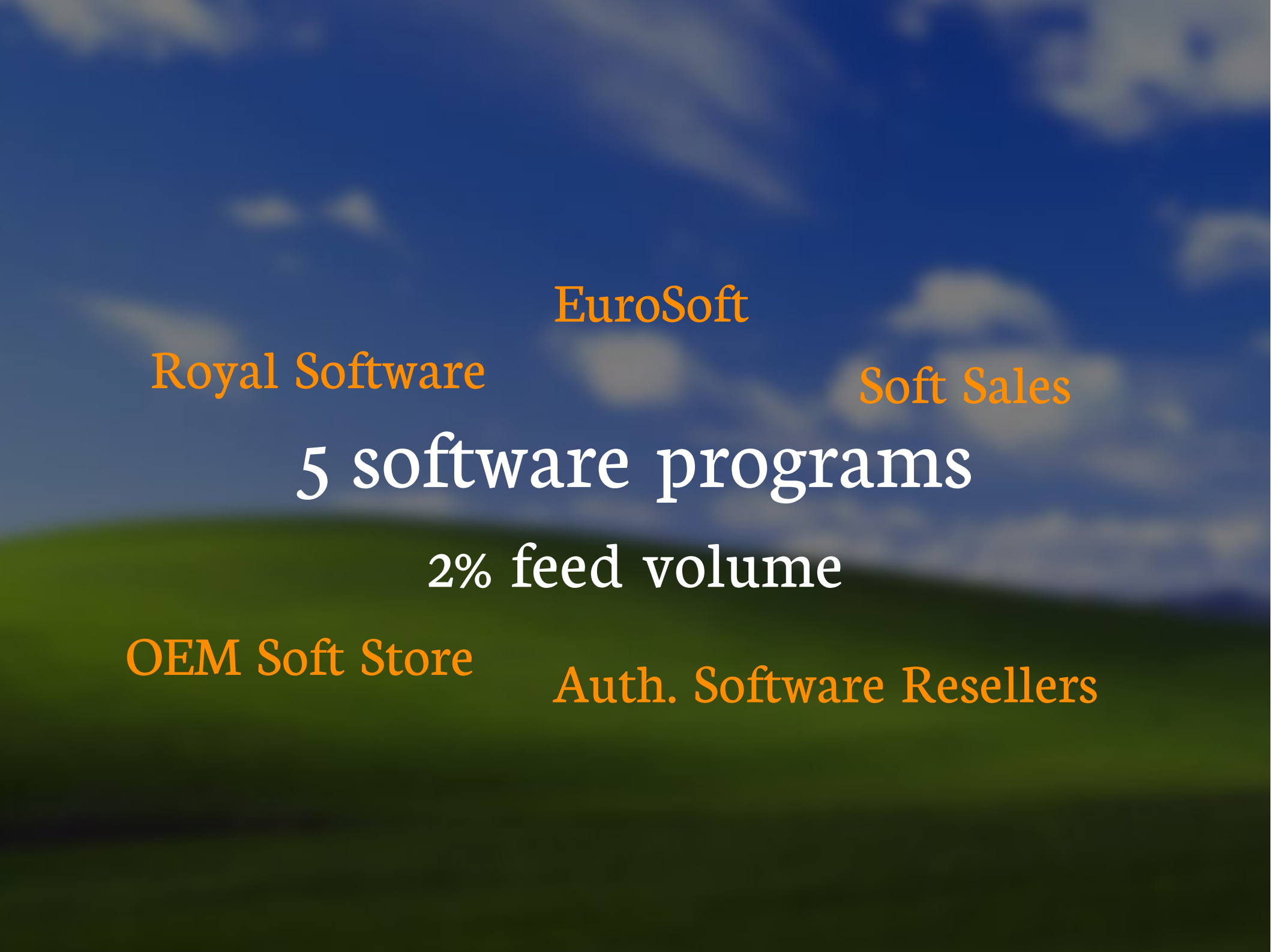


- Aug 1 -- Oct 31 2010
- 6 URL/Spam feeds + our own spam mill
- 968M URLs
  - 10% unique
  - 17M domains
  - 15M URLs web-crawled
  - 100+ Firefoxes
  - EC2 and other /24s
- Coverage: 98% of URLs use domains we crawled
- Pharma, replicas, software

Affiliate programs


Pharmacy Express
Stud Extreme
ED Express
Online Pharmacy
UltimatePharmacy
Stallion
DrugRevenue
GlavMed
ManXtenz
HerbalGrowth
RX Promotion
RX Partners
Dr. Maxman
30 pharma programs
MaxGentleman
93% feed volume
VigREX
EvaPharmacy
Stimul-cash
Swiss Apotheke
MAXX Extend
US HealthCare
Canadian Pharmacy
Virility
Viagrow
World Pharmacy
PH Online


Ultimate Replica
Distinction Replica
Exquisite Replica
Diamond Replica
Prestige Replica
One Replica
10 replica programs
5% feed volume
Luxury Replica
Watch Shop
Aff. Accessories
Swiss Rep. & Co.


EuroSoft
Royal Software
Soft Sales
5 software programs
2% feed volume
OEM Soft Store
Auth. Software Resellers

Purchasing

Purchasing protocol

- Two+ purchases per affiliate program
  - 120 attempts, 76 authorizations, 56 settled
  - 49 deliveries
- From IP address near delivery address
- Via VISA prepaid cards, friendly issuer
- With unique card per purchase
- To private addresses and PO Box


Purchase Meister
Project Lead

GLOBAL EXPRESS MAIL
UNITED STATES POSTAL SERVICE®

Arrival
For Exchange Office use only

AMC of Arrival | Dispatch Number

SFO | 5349

02FEB10 | CN

EMS

Addressee Copy
For Inbound EMS Items Only

Item Number

EE248975418CN

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

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

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

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

PS Form 5626X, October 2002

Deliver By 3:00 PM Today

速递服务专家

EMS


EXPRESS MAIL
DECLARATION EN DOUANE
MEDICINE


351 A
ENCLOSED
880654
USA


20
30
40
50
SUBMARINER
SUPERLATIVE CHRONOMETER
OFFICIALLY CERTIFIED


POLFY
16610


ROLEX
16610

< $280 per program

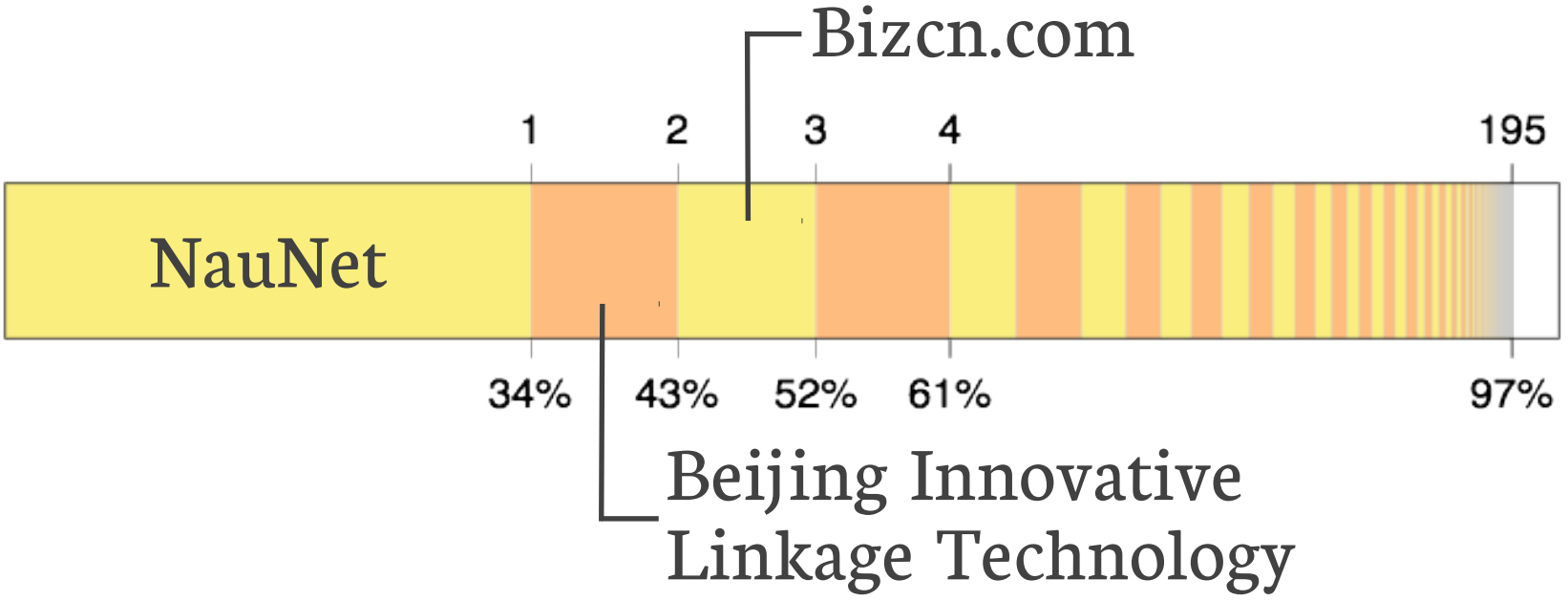
~$5,000 total

Bottlenecks

Registrars

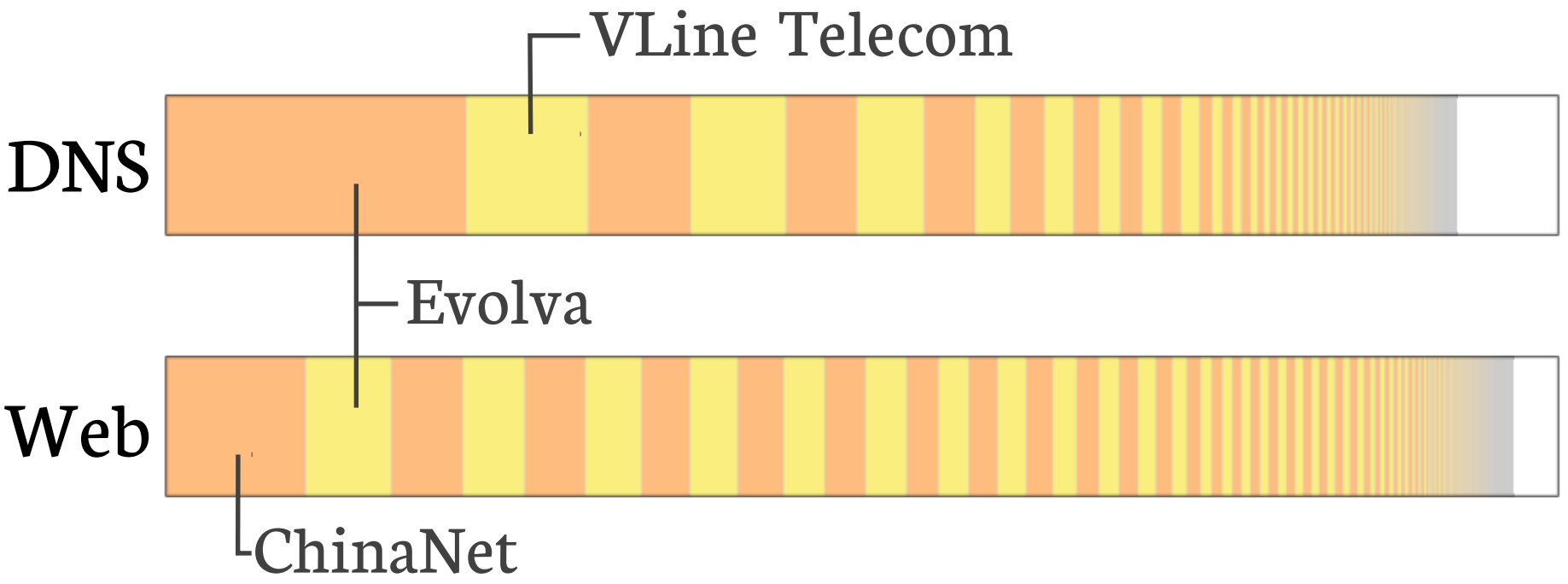
← All pharma, replica, software spam →

Registrars



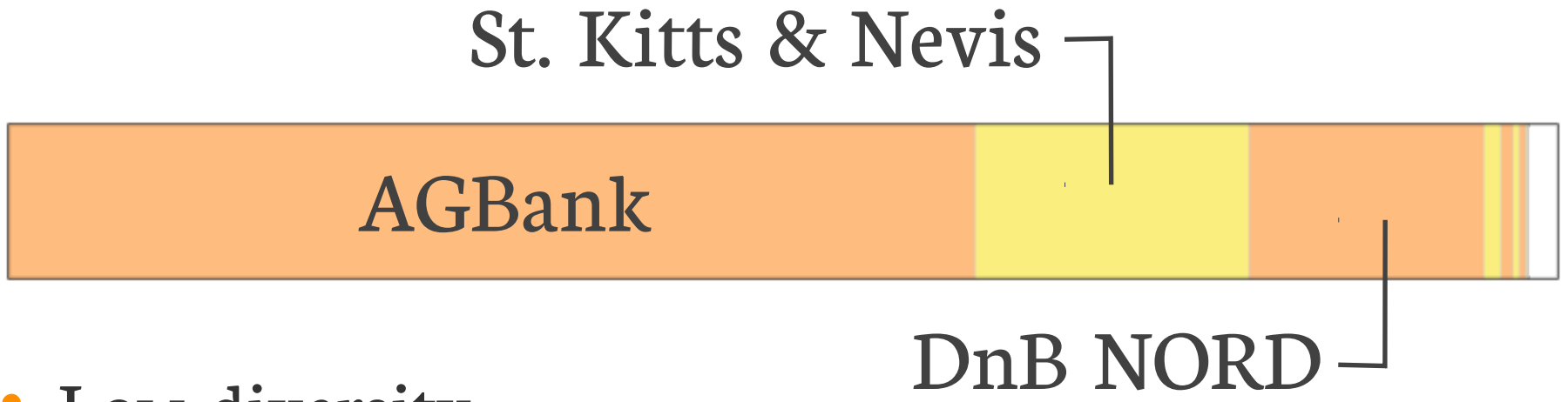
- Some concentration in NauNet (Russia)
- Lots of diversity in remaining domains
- Very low switching cost

DNS & Web hosting



- Even more diversity than with registrars
- Again low switching cost

Merchant banks



- Low diversity
  - 3 banks cover 95% of spam
  - Few banks are willing to work with risky merchants
- High switching cost
  - In-person account creation, due diligence
  - Multi-day process

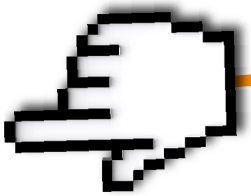

AGBANK
ATM

Targeting the bottleneck

- Takedown approach: slow
  - Shame merchant banks into dropping merchants
  - Activity not always illegal in local country
- Blacklist approach: faster
  - Issuing banks refuse to settle certain transactions
    - E.g. card-not-present for certain merchant categories
  - Quick blacklist update
  - Quick merchant bank switch detection
  - Precedent in gambling industry (UIGEA)

Summary

- Click trajectories
  - Target weakest link in end-to-end value chain
  - ~1B URLs, 45 affiliate programs, 120 purchases
  - 3 banks cover 95% of credit card transactions
- Payment processing is a promising bottleneck
  - 2 possible intervention strategies
- Encouraging feedback
  - From banks and spammers :)



Recent developments

- Continued purchase-driven monitoring
  - ~700 orders, ~500 completed, ~30 banks
  - Commercial take-downs
  - Program reaction: purchase screening, evasions
  - Affiliate business severely hurt
- Ground truth
  - Database dumps of 2 programs, covering $170M
  - Top affiliates make > $1M / year
  - Programs turn 10-20% of revenue into profit
    - RXP: $7.8M revenue in 6 months, $1.3M profit

Thanks!

christian@icir.org

@ckreibich