Spam Economics

Vern Paxson

EECS Department, University of California
International Computer Science Institute
Berkeley, California USA
vern@cs.berkeley.edu

November 27, 2012

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Chris Kanich* Christian Kreibich† Kirill Levchenko* Brandon Enright*
Geoffrey M. Voelker* Vern Paxson† Stefan Savage*

†International Computer Science Institute
Berkeley, USA
christian@icir.org,vern@cs.berkeley.edu

*Dept. of Computer Science and Engineering
University of California, San Diego, USA
{ckanich,klevchen,voelker,savage}@cs.ucsd.edu
bmenrigh@ucsd.edu

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*

*Department of Computer Science and Engineering
University of California, San Diego

†Computer Science Division
University of California, Berkeley

◇International Computer Science Institute
Berkeley, CA

‡Laboratory of Cryptography and System Security (CrySyS)
Budapest University of Technology and Economics

Motivation

Are Botmasters & Spammers the New Drug Lords?

Storm worm 'making millions a day'

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

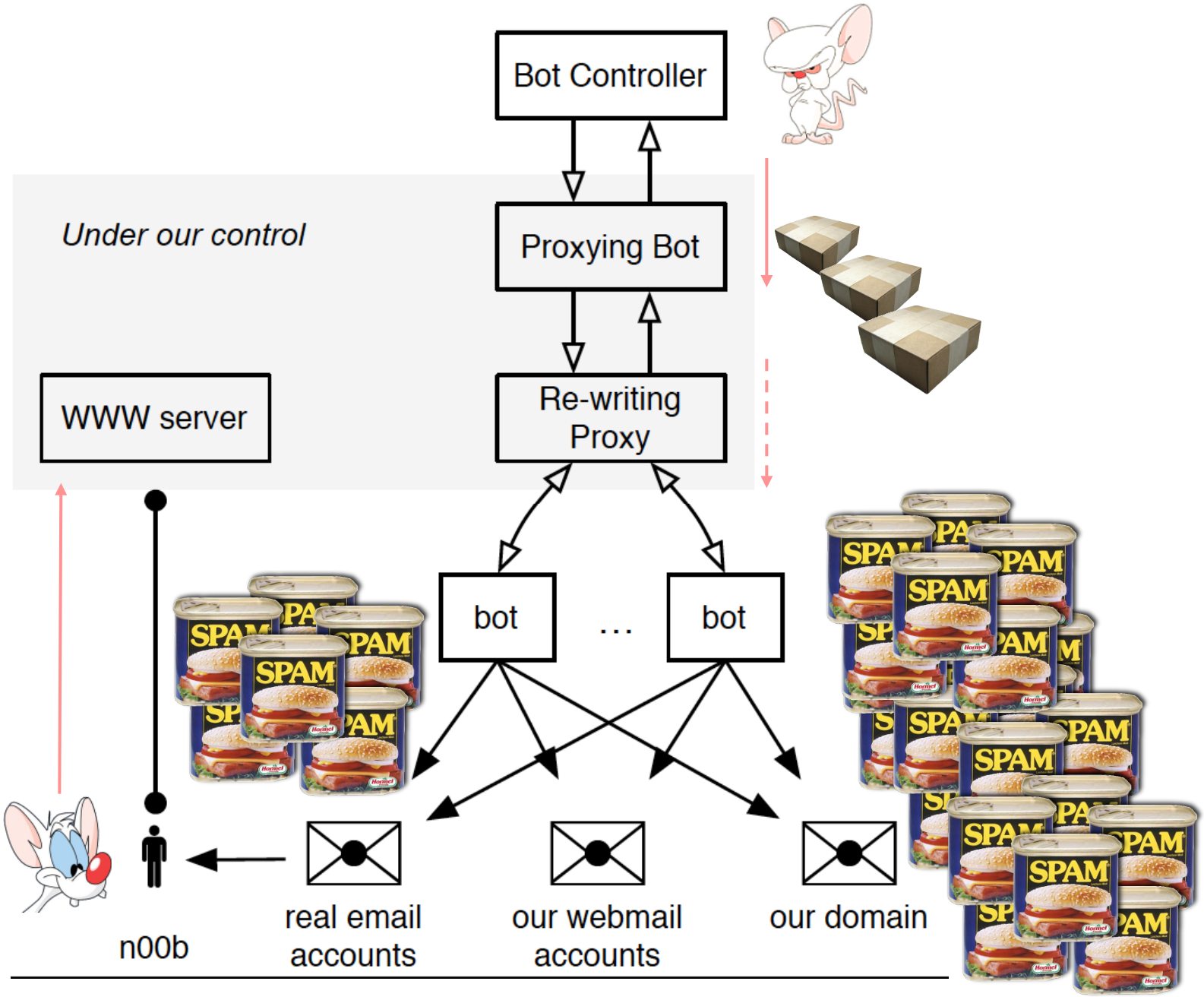
Clive Akass, Personal Computer World 11 Feb 2008

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.

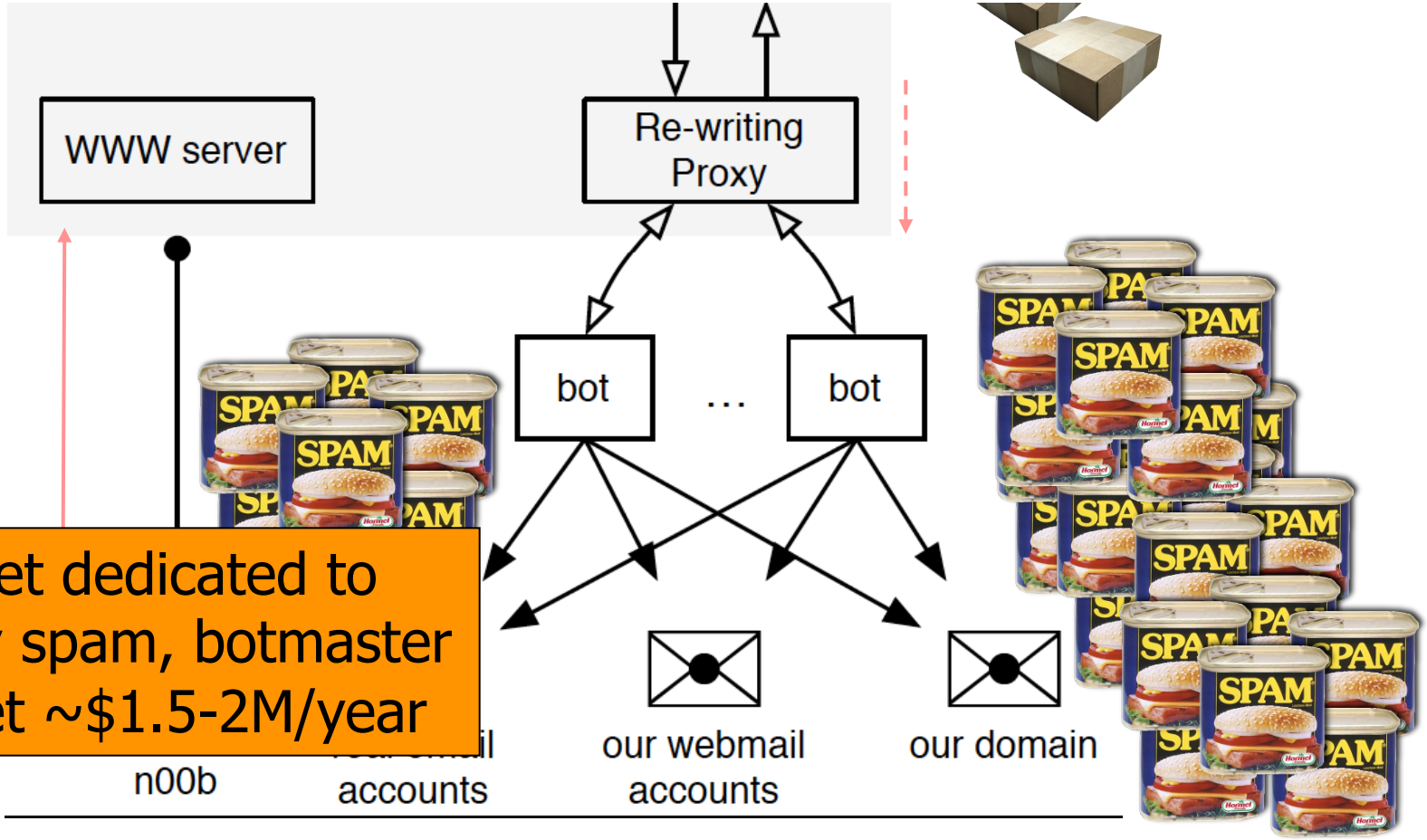
Joshua Corman, of **IBM Internet Security Systems**, said that in the past it had been assumed that web security attacks were essential ego driven.

How can we **measure** this? Seemingly only knowable by the spammers themselves.

- Spam finance elements:
  - Cost-to-send vs. Profit-per-response
  - Key missing element: spams-needed-per-response, i.e., *conversion rate*

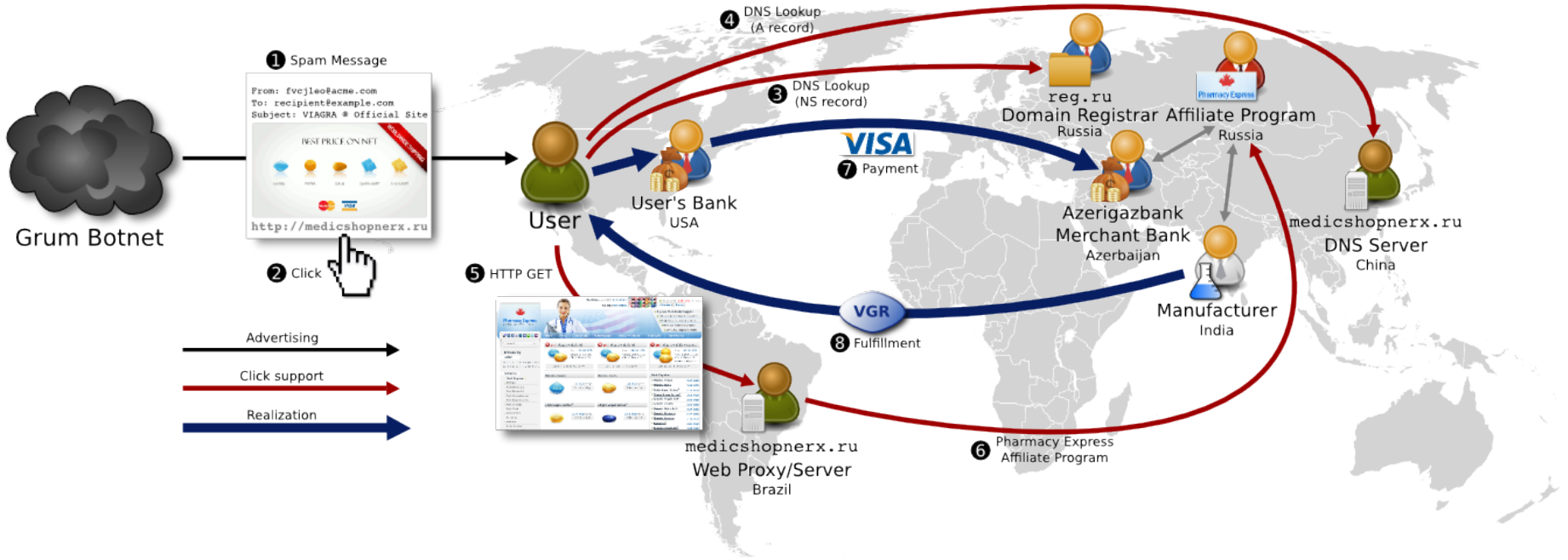

Bot Controller
Under our control
Proxying Bot
WWW server
Re-writing Proxy
bot
…
bot
real email accounts
our webmail accounts
our domain
n00b

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%



If botnet dedicated to pharmacy spam, botmaster could net ~$1.5-2M/year

Phases of the Spam Value Chain



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

Feed Name	*Feed Description*	*Received URLs*	*Distinct Domains*
Feed A	MX honeypot	32,548,304	100,631
Feed B	Seeded honey accounts	73,614,895	35,506
Feed C	MX honeypot	451,603,575	1,315,292
Feed D	Seeded honey accounts	30,991,248	79,040
Feed X	MX honeypot	198,871,030	2,127,164
Feed Y	Human identified	10,733,231	1,051,211
Feed Z	MX honeypot	12,517,244	67,856
Cutwail	Bot	3,267,575	65
Grum	Bot	11,920,449	348
MegaD	Bot	1,221,253	4
Rustock	Bot	141,621,731	13,612,815
Other bots	Bot	7,768	4
Total		968,918,303	17,813,952

Table I: Feeds of spam-advertised URLs used in this study. We collected feed data from August 1, 2010 through October 31, 2010.

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

Covered all the major

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

PAIN RELIEF
- Vicodin ES
- Hydrocodone
- Percocet
- Lortab
- Darvocet (Proxyvon)
- Codeine
- **View all products**

ANTI-ANXIETY
- Xanax
- Valium (® ROCHE)
- Ativan (® Wyeth)
- Klonopin (generic)
- Valium (generic)
- Anti-Anxiety Pack
- Atarax
- **View all products**

ADHD Treatment
- Adderall
- Brand Ritalin
- **View all products**

WEIGHT LOSS
- Phentermine

Order approved

Your transaction has been approved.

Your order ID: 138730
First name: Geoff
Last name: Voelker
Card used with this order: 46*****2205
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:
==========
medissue.com +12175686119
==========

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

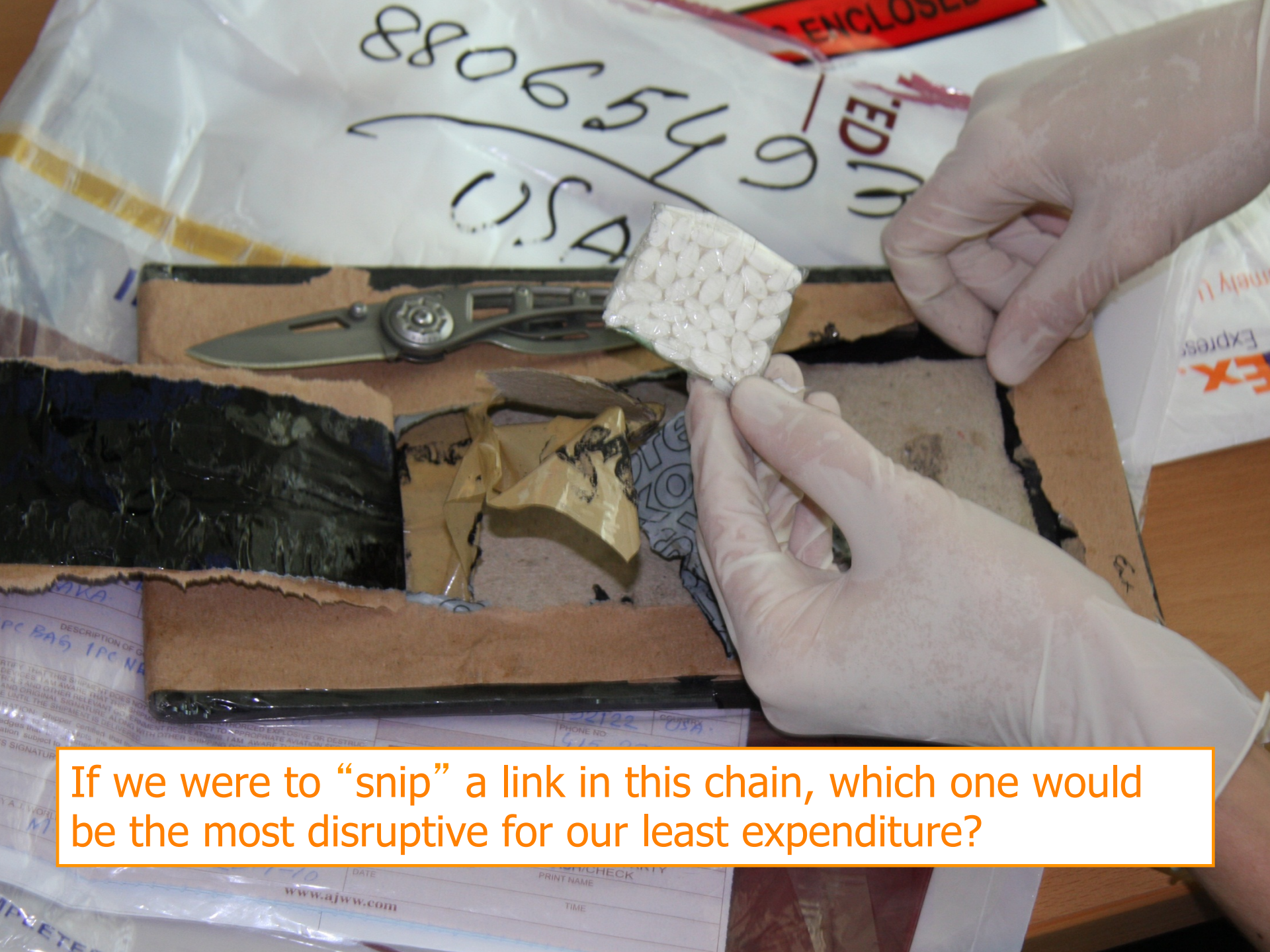
ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

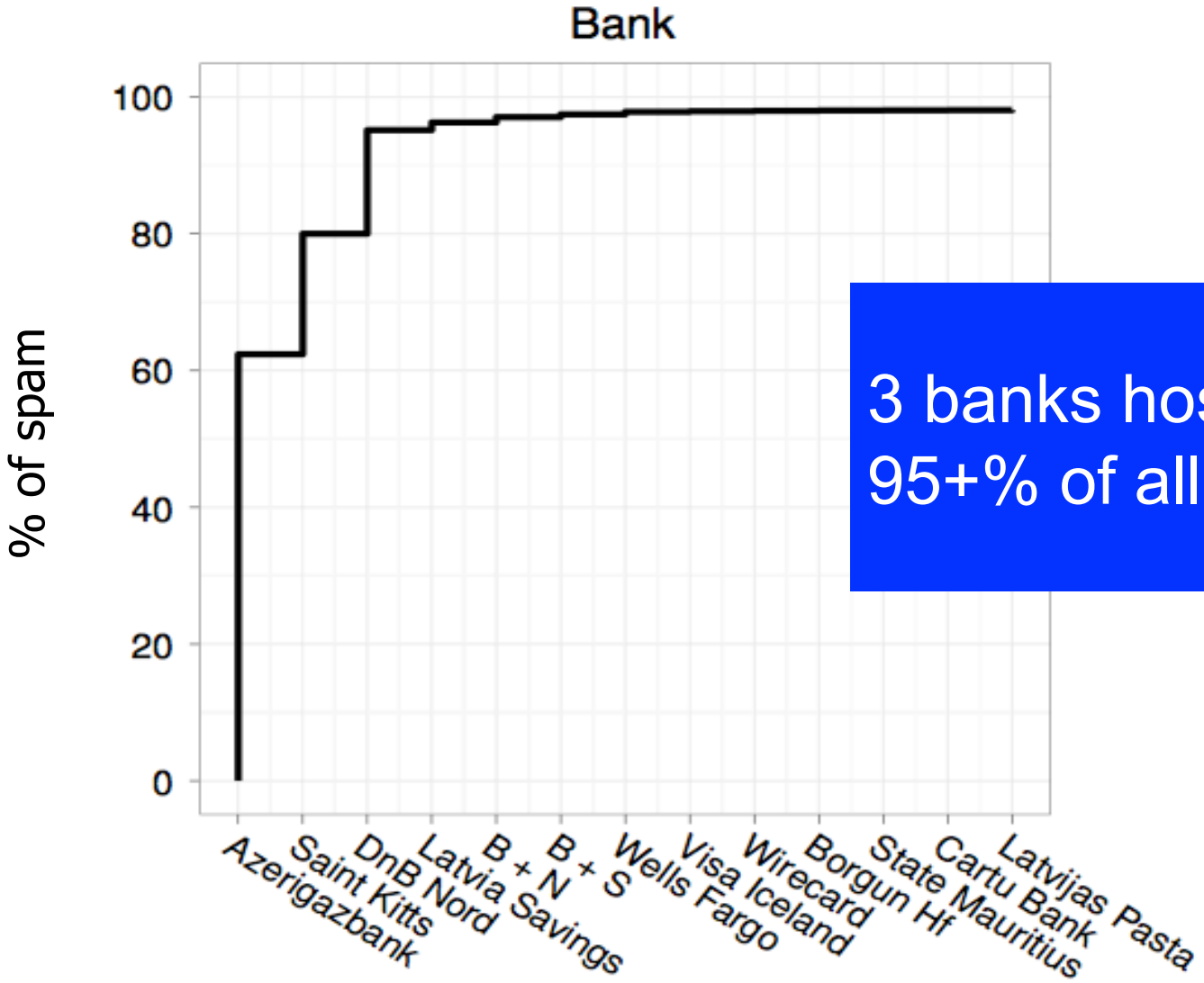
Dear **Geoff Voelker**, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com


SEALED FOR YOUR PROTECTION
vpXl
#1 Dietary Supplement for Men
100% Natural Dietary Supplement
Contains 60 capsules

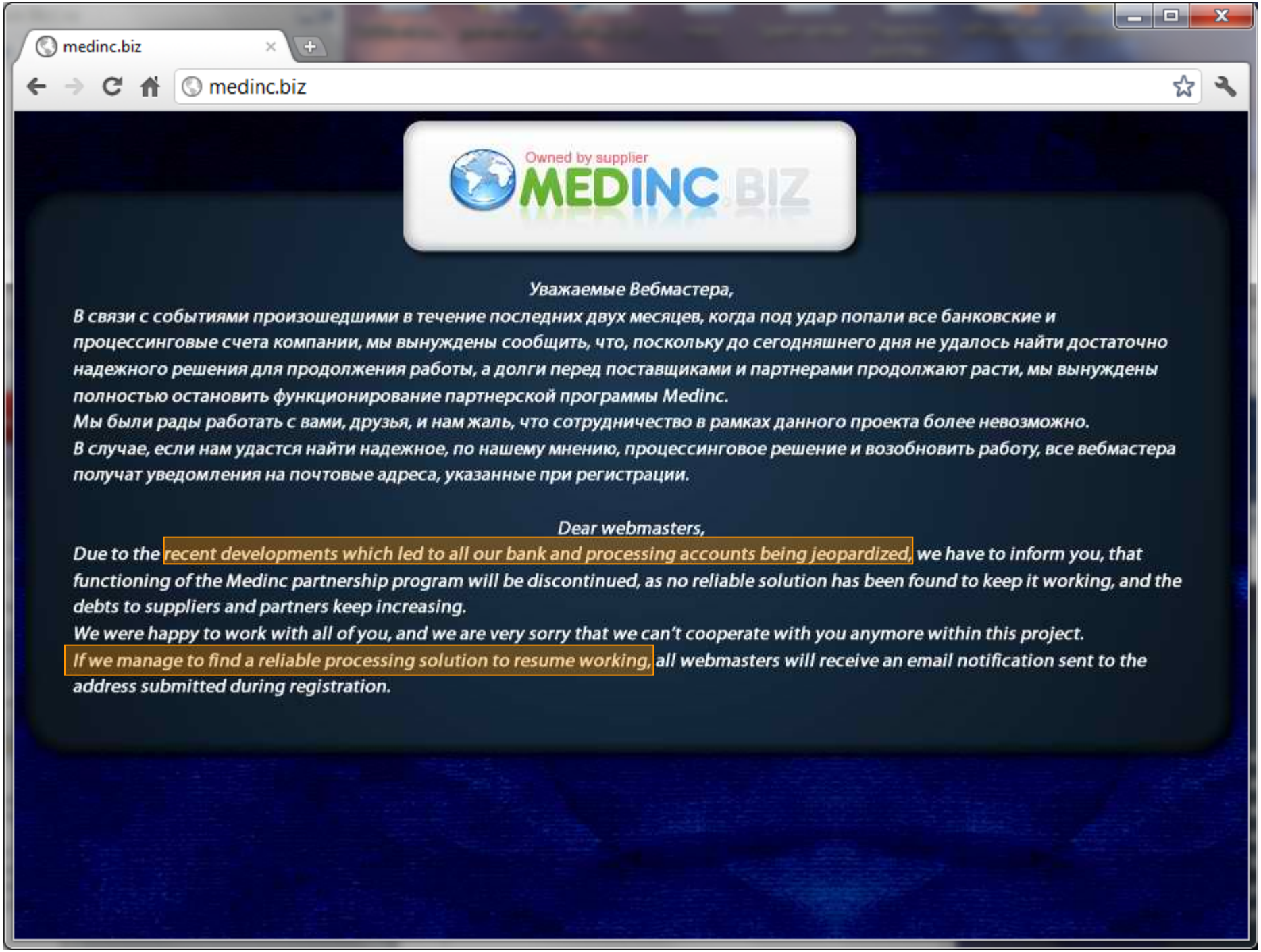

If we were to “snip” a link in this chain, which one would be the most disruptive for our least expenditure?

Merchant Bank bottlenecks



3 banks hosted
95+% of all sales

Findings Lead to a Wealth of Relationships …


medinc.biz
medinc.biz
Owned by supplier
MEDINC.BIZ
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.