Perspectives on Security as an Empirical Science

Vern Paxson

Electrical Engineering & Computer Sciences
University of California, Berkeley
International Computer Science Institute
vern@berkeley.edu

January 23, 2015

Overview

- Why we want a *Science of Cyber-Security*
- Why it's challenging to attain
- The nature of empirical science as it relates to security
  - Research culture, reproducibility
  - Sure would be good to have data …
- The power of holistic analyses …
  - … and *opportunism*
  - … and *meta-empiricism*

Why Science?

Why We Want a *Science of Cyber-Security*

Why We Want a *Science of Cyber-Security*

- Surely there's some way to get a handle on the incessant threats we face … ?

- Science = prediction + control
  - … via apt understanding/modeling

What Do We Mean By “Science”?

1. Characterize
2. Hypothesize
3. Predict
4. Experiment
5. Analyze
6. Repeat …

What Do We Mean By “Science”?

1. Characterize
2. Hypothesize
3. Predict
4. Experiment
5. Analyze
6. Repeat …

1. Disseminate
2. Independently confirm

What Do We Mean By “Science”?

1. Characterize
2. Hypothesize
3. Predict
4. Experiment
5. Analyze
6. Repeat …

1. Disseminate
2. Independently confirm

All with a degree of ***rigor***.
But varies *hugely* with problem domain:

e.g. keystroke biometrics

vs.

cybercrime payment disruption

STAND BACK

I'M GOING TO TRY

SCIENCE

But What Kind of Science? (*S. Savage*)

- **Like math**:
  - Has an axiomatic basis, once you derive principals and implement them, everything will be secure (e.g., *crypto*)
- **Like a physical science** (e.g., experimental physics):
  - There is real Platonic truth and we can discover it by generalizing from experimental evidence (e.g., *biometrics*)
- **Like war-fighting/criminology**:
  - There is an adversary innovating ways to outsmart us and we must react, anticipate and out innovate them
- **Like engineering**: functionality vs. cost/time/effort
- **Like a social science** (e.g., sociology/economics):
  - There are contextual truths discoverable via experiments / field work, and some of them might be generalizable

NSF Proposal

TWC: Frontier: Collaborative:
Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Stefan Savage, Geoffrey M. Voelker, James Fowler, Alex Snoeren,
Lawrence Saul, Kirill Levchenko, Erin Kenneally
University of California, San Diego

Vern Paxson, Mark Allman, Chris Grier, Chris Hoofnagle, Dan Klein,
Christian Kreibich, Deirdre Mulligan, Nicholas Weaver
International Computer Sciences Institute

Damon McCoy
George Mason University

September 2012 – August 2017

Why An Empirical Science?

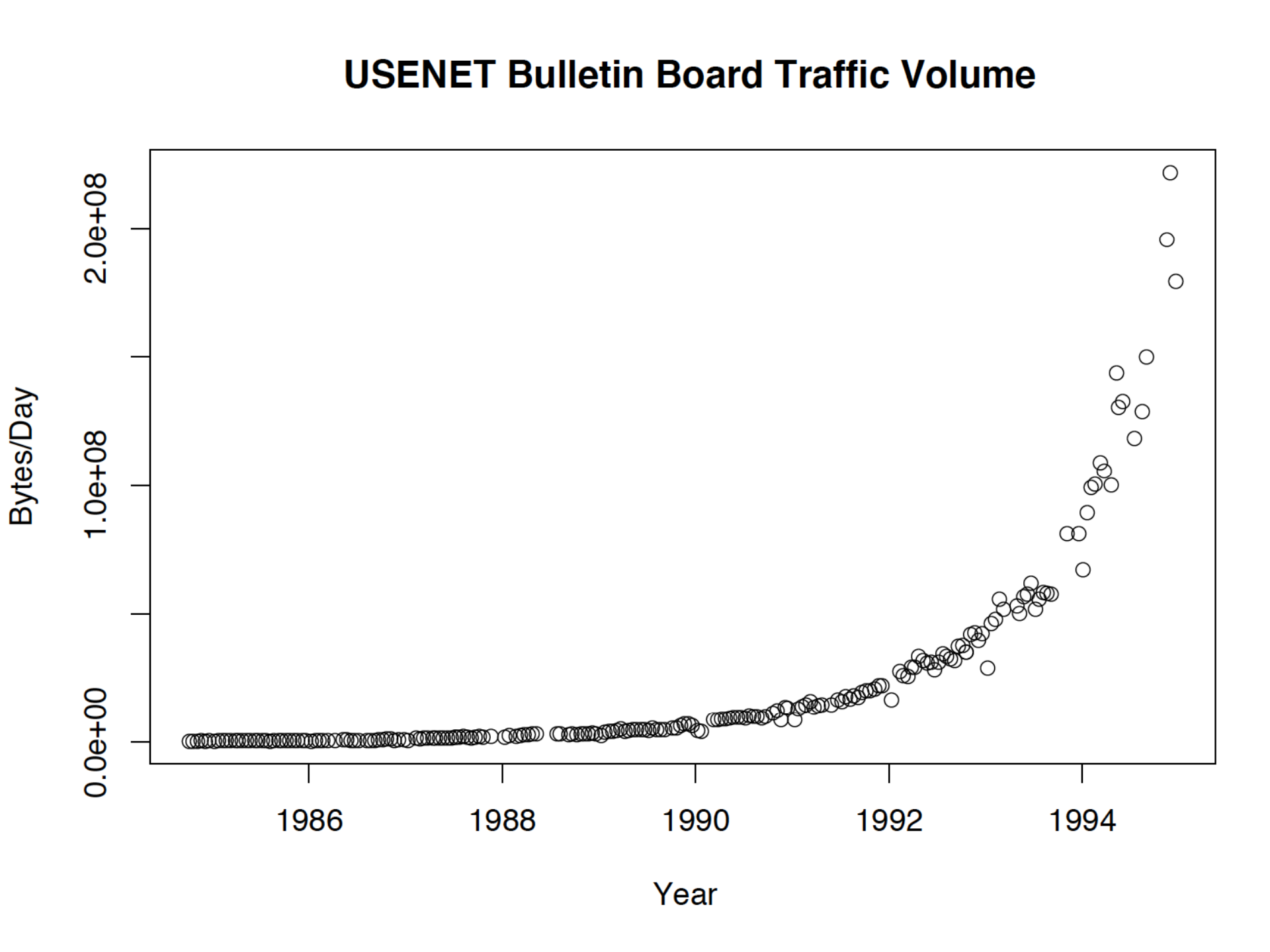
Why An Empirical Science?

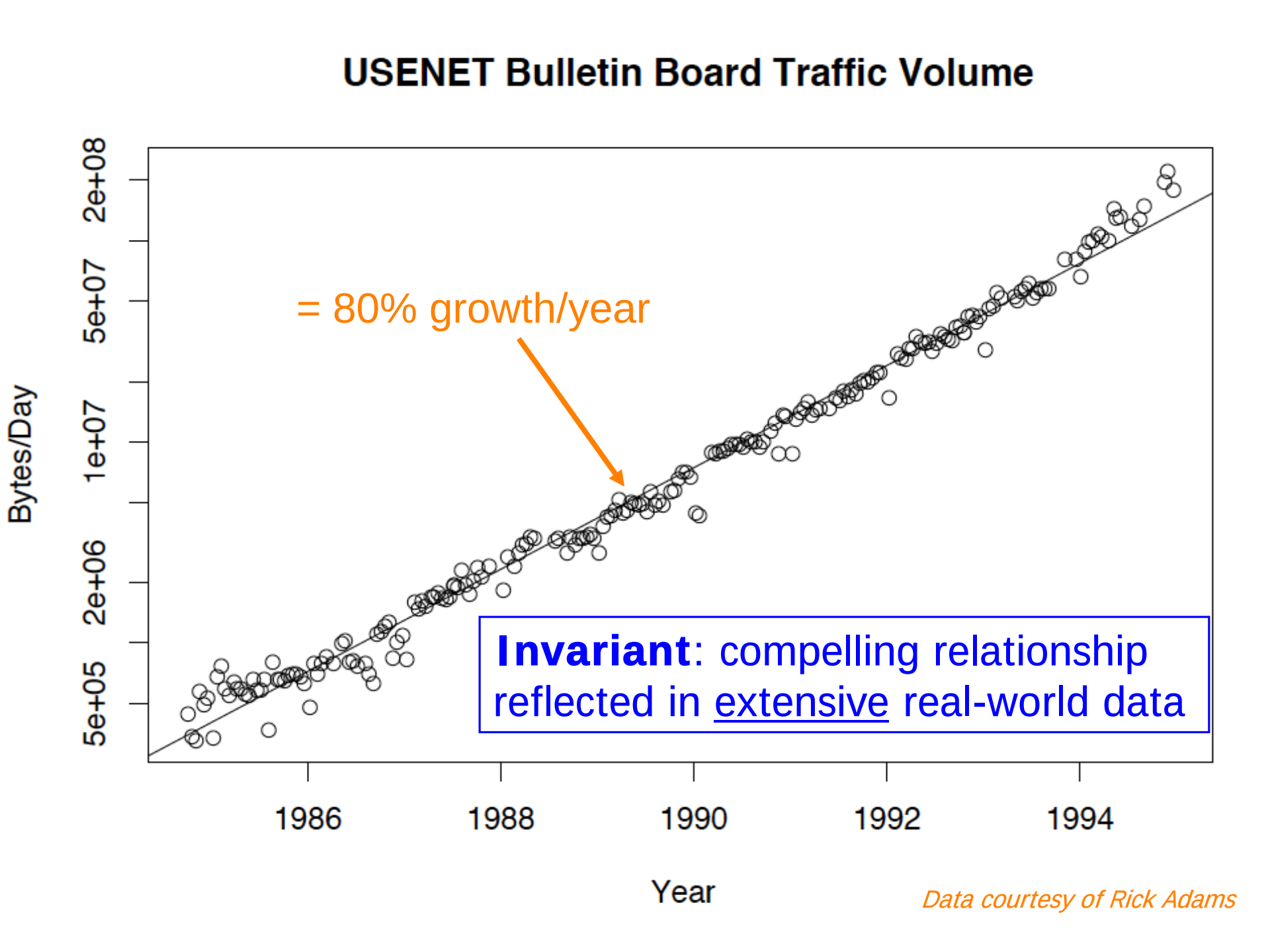
Perspective #1:
Boy do things change fast …

Why An Empirical Science?

Perspective #1:
Boy do things change fast …

Consider an analogy: Networking

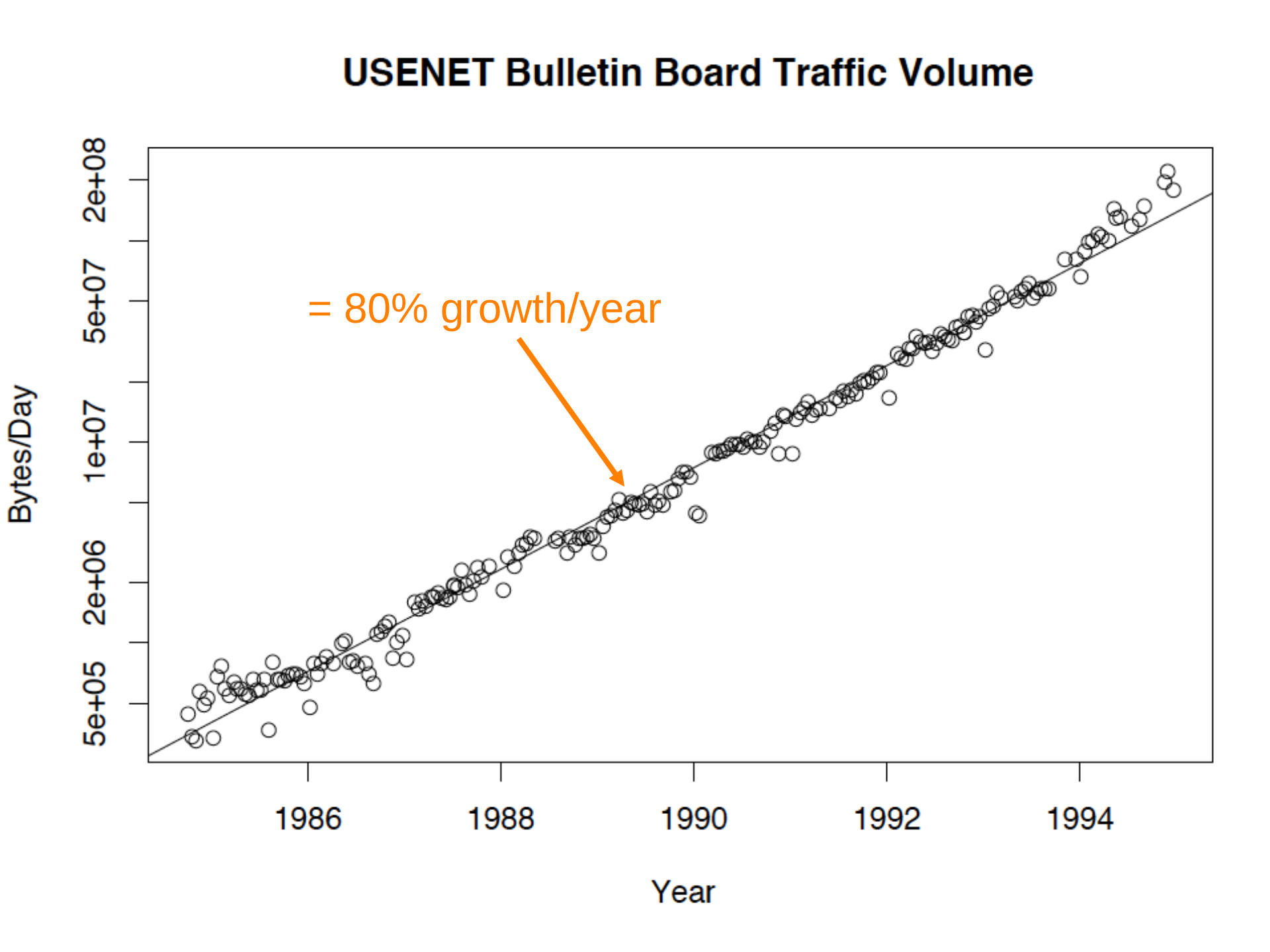

USENET Bulletin Board Traffic Volume
Bytes/Day
0.0e+00
1.0e+08
2.0e+08
1986
1988
1990
1992
1994
Year

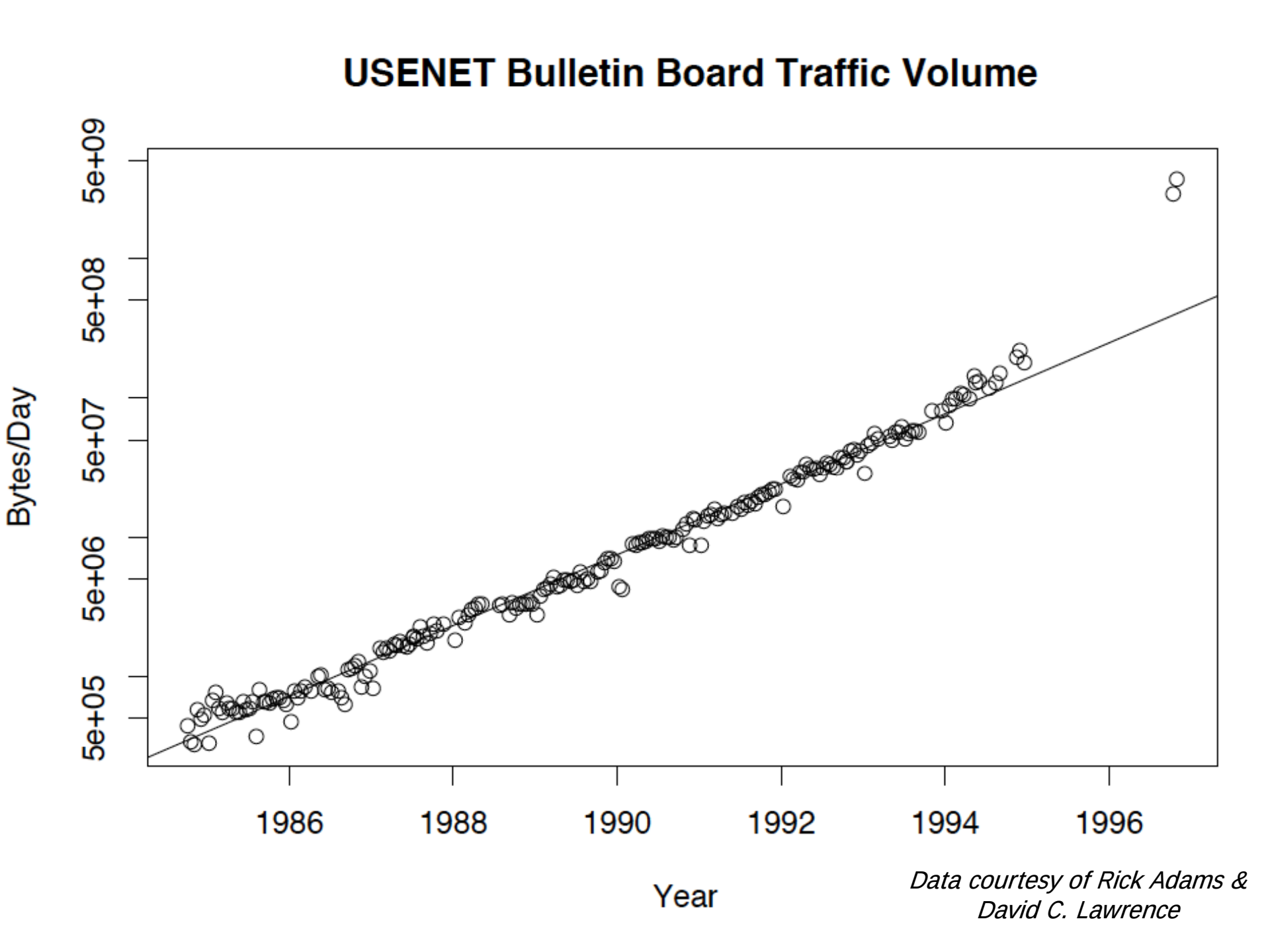

USENET Bulletin Board Traffic Volume
Bytes/Day
5e+05
2e+06
1e+07
5e+07
2e+08
1986
1988
1990
1992
1994
Year
= 80% growth/year
Invariant: compelling relationship reflected in extensive real-world data
Data courtesy of Rick Adams

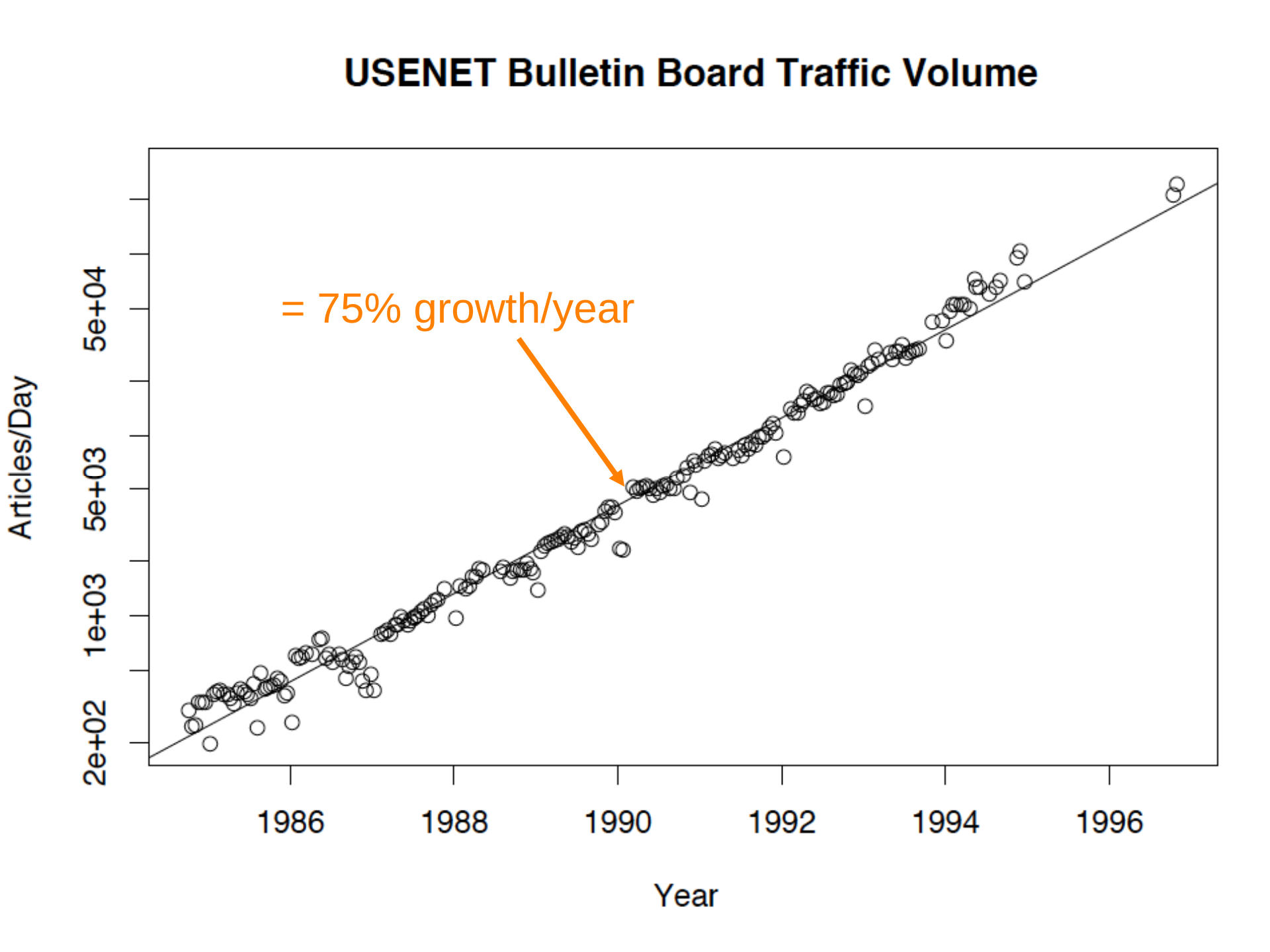
Why An Empirical Science?

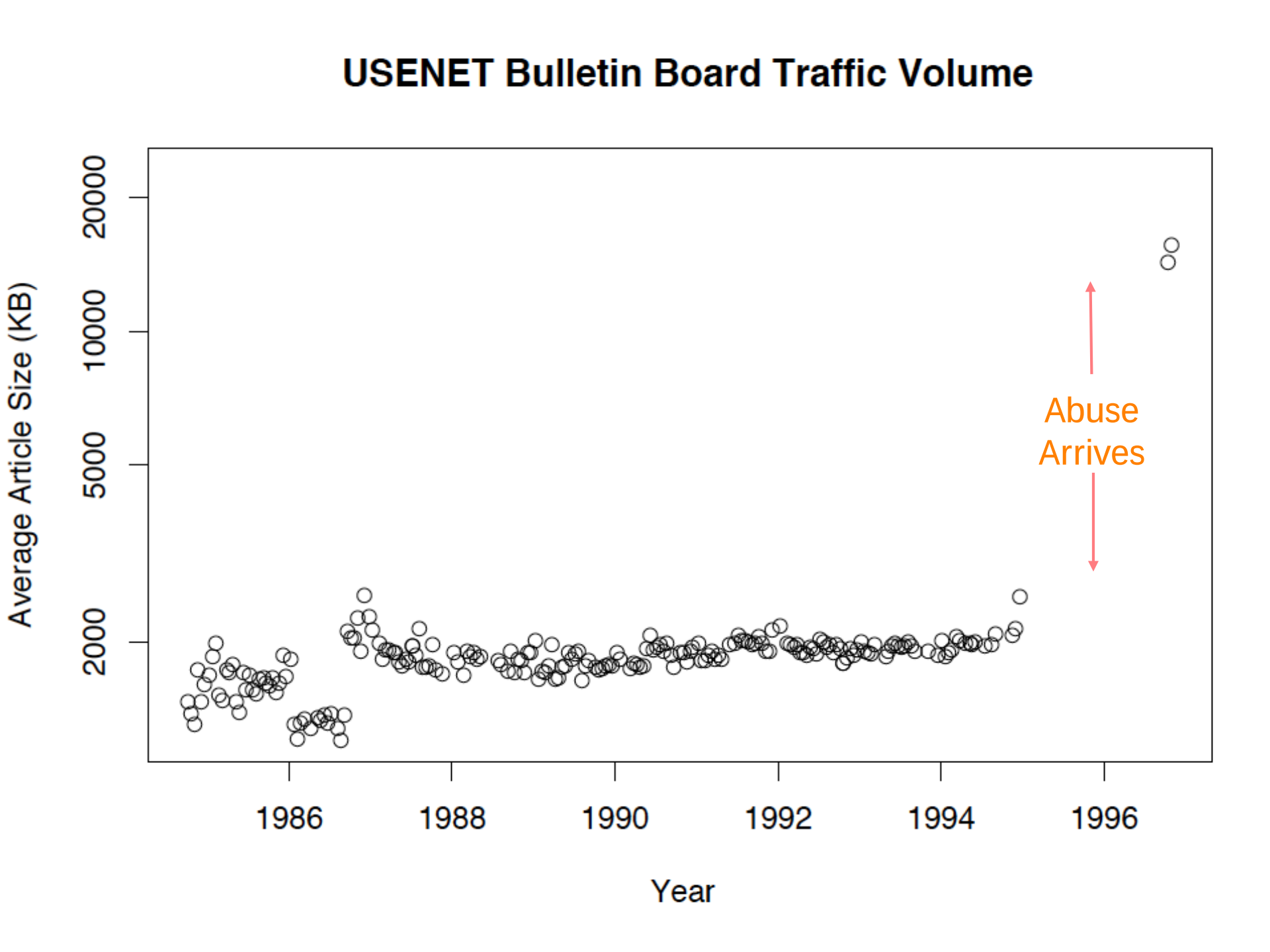
Perspective #1:
Boy do things change fast …

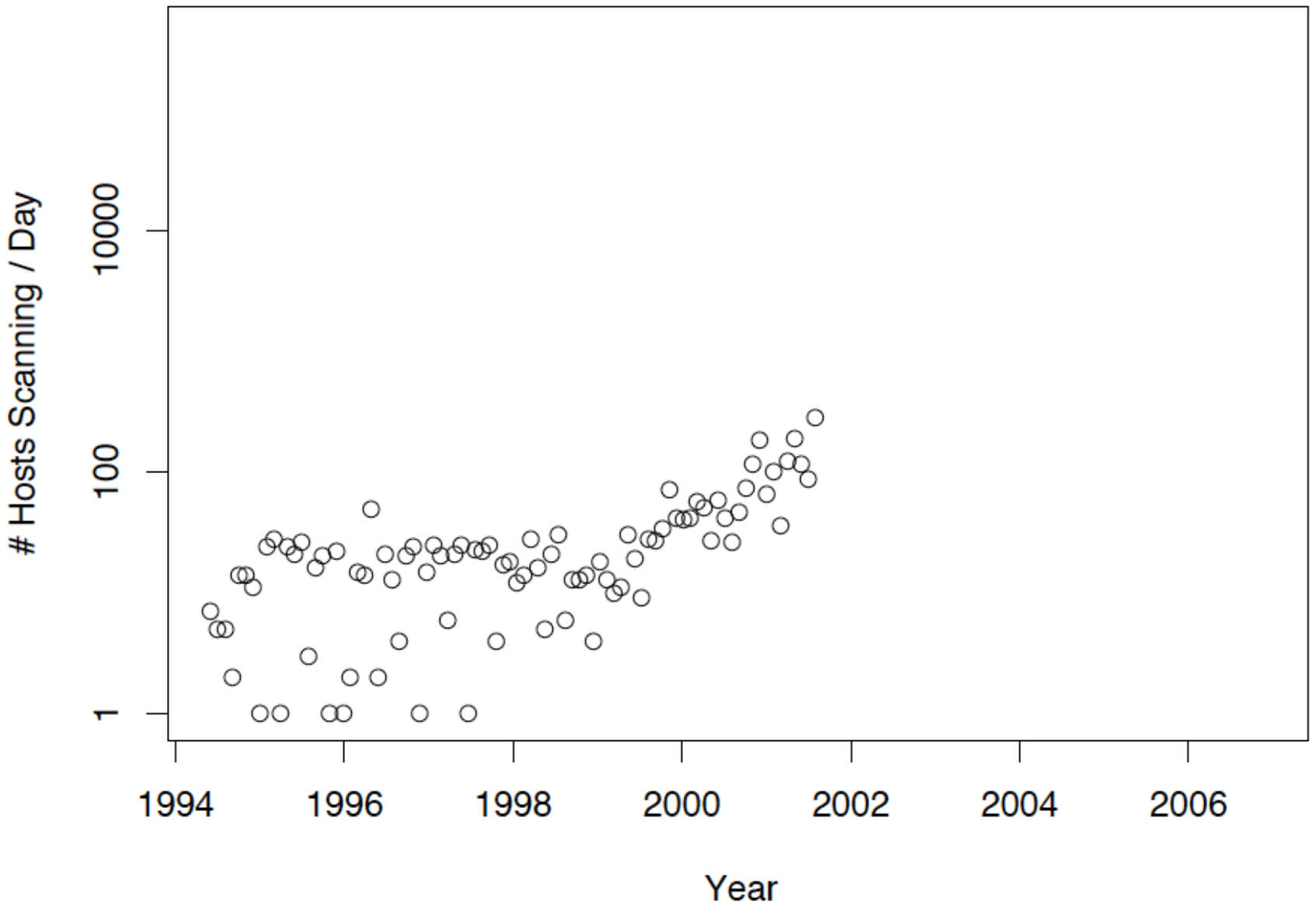
Perspective #2:
Boy they change even faster …

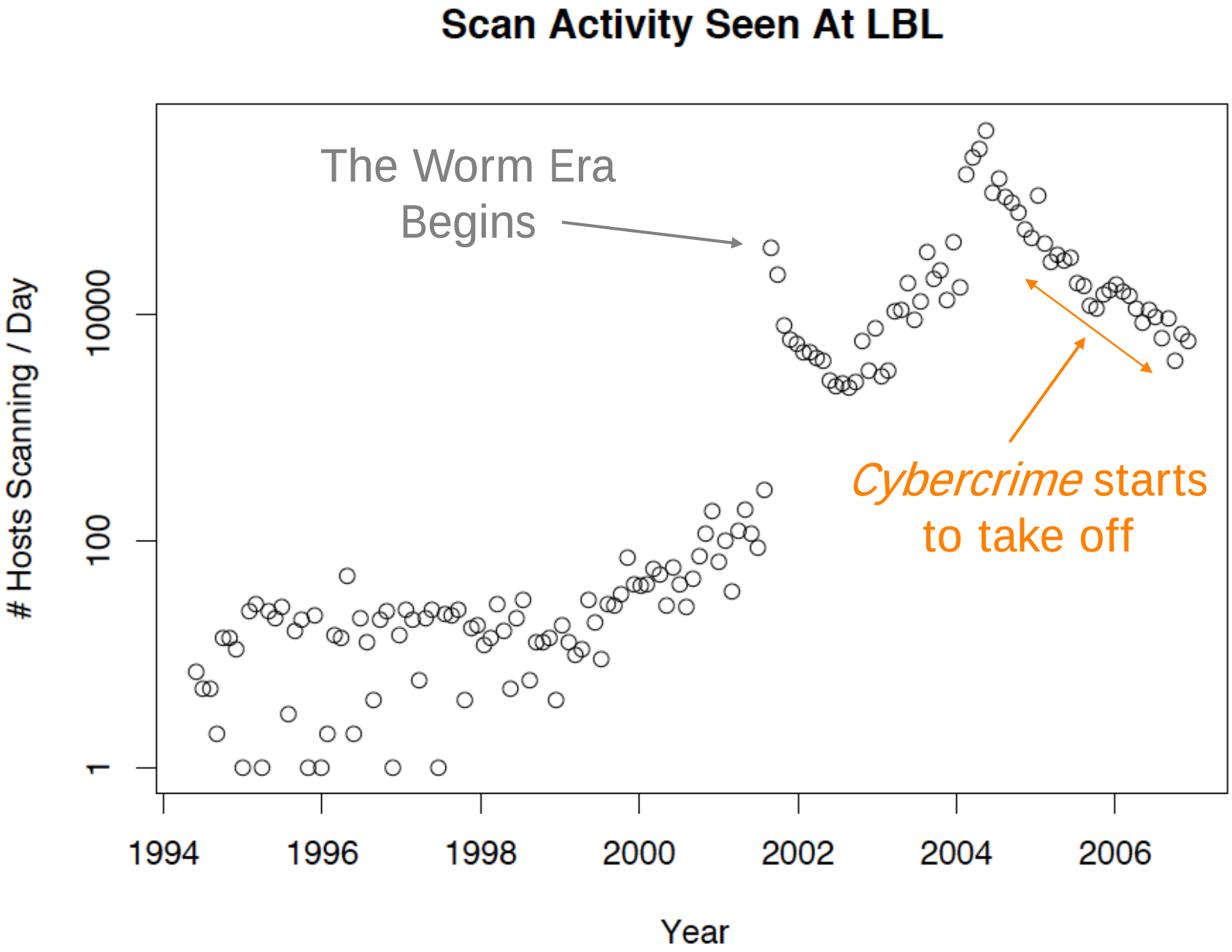

USENET Bulletin Board Traffic Volume
= 80% growth/year
Bytes/Day
5e+05
2e+06
1e+07
5e+07
2e+08
1986
1988
1990
1992
1994
Year


USENET Bulletin Board Traffic Volume
Bytes/Day
5e+05
5e+06
5e+07
5e+08
5e+09
1986
1988
1990
1992
1994
1996
Year
Data courtesy of Rick Adams &
David C. Lawrence


USENET Bulletin Board Traffic Volume
= 75% growth/year
Articles/Day
2e+02
1e+03
5e+03
5e+04
1986
1988
1990
1992
1994
1996
Year


USENET Bulletin Board Traffic Volume
Average Article Size (KB)
2000
5000
10000
20000
1986
1988
1990
1992
1994
1996
Year
Abuse
Arrives


Scan Activity Seen At LBL
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year


Scan Activity Seen At LBL
The Worm Era Begins
Cybercrime starts to take off
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year

Observations of the Problem Domain

Data Issues

- Where do security empiricists get data?
- Hugely sensitive & difficult to anonymize
  - De facto standard: handshake deals / collaborations
- Attacks = easy part; **background** = hard part
- Major **ground truth** issues
- Hugely complicates desire for reproducing results
- Analogous issues arise for *deep validation*
  - How to test new approaches in realistic settings?
- Makes us opportunists

Invariants & Time Scales

- How quickly does the landscape change?
- For research purposes, one key time constant is invariants that hold for ≥ 5 years
  - i.e., Ph.D. dissertation

- Given these are rare,
  How important is reproducibility?

Why Is This Harder than Hard Science?

- Our environment not only continually evolves, but does so guided by intelligence
- Secure systems have to deal with events that occur with *probability of measure zero*
  - (John Doyle, Cal Tech)

Why Is This Softer than Hard Science?

- Both the adversaries and targets are **human**
- Salient issues are: *behavior*, *motivation*, *relationships*, *incentives/economics*, *perceptions*, *values* (S. Savage)
- Where do our invariants come from?
  - Intelligent opponents fundamentally imply **change**
- OTOH, in some ways people don't change …

Axiom of Criminal Laziness

Cybercrooks will work energetically to sustain their current cash flow …

… but will not look out strategically beyond it to serve their long-term interests.

The Power of Holistic Analyses …
… and Opportunism

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

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

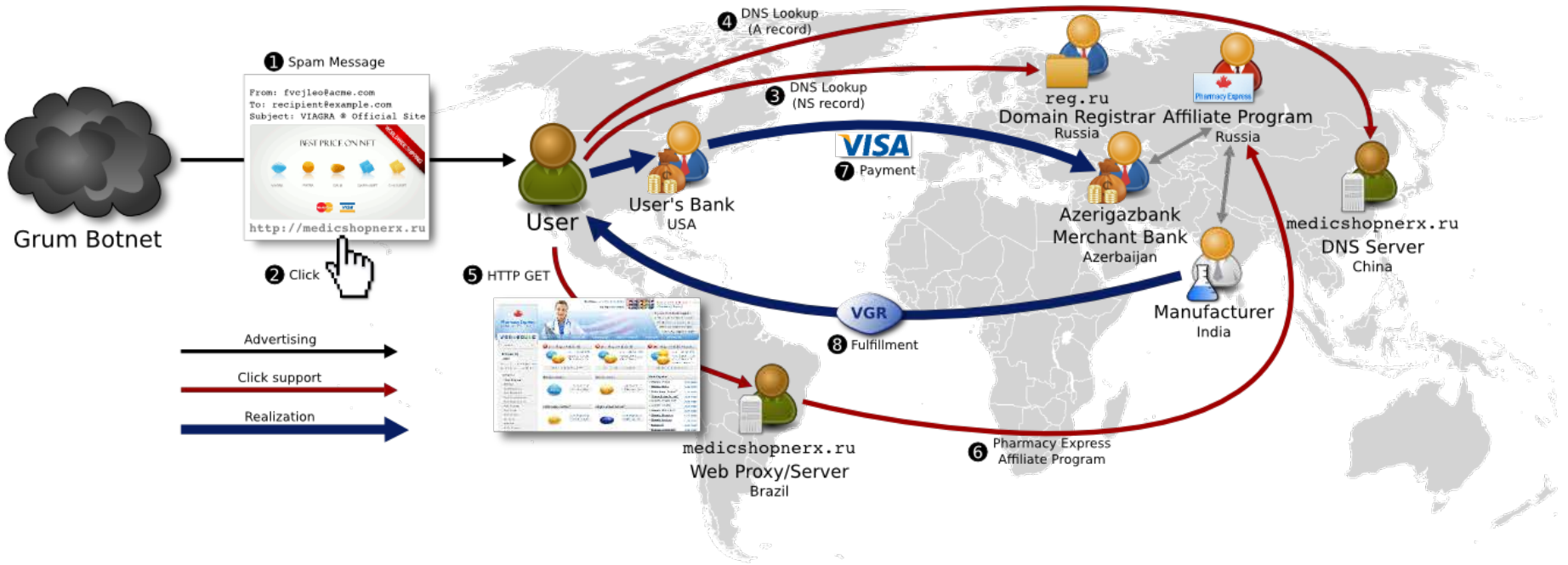
Viagra Professional

Our price
$3.73

More info | Add to cart

Done

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?

Measuring URLs, DNS servers, HTTP redirection, etc. all a matter of energetic *crawling & recording*.

But **merchant banks** / **Visa** / "**fulfillment**" ?

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: 138731
First name: Kirill
Last name: Levchenko
Card used with this order: 46*****2288
Total amount charged: $52.95

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.

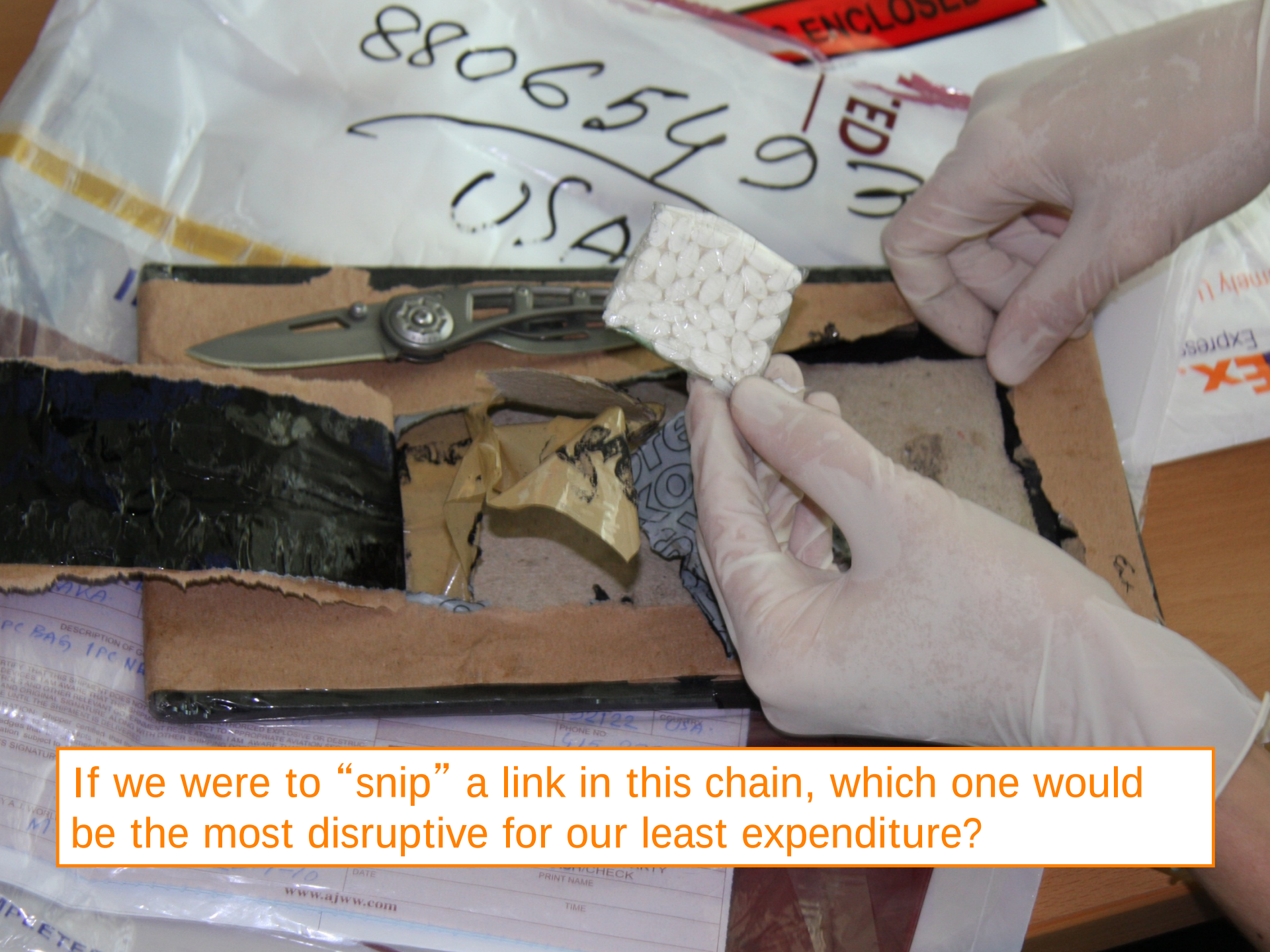
ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear **Kirill Levchenko**, 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?

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 New York Times

The Opinion Pages

EDITORIAL

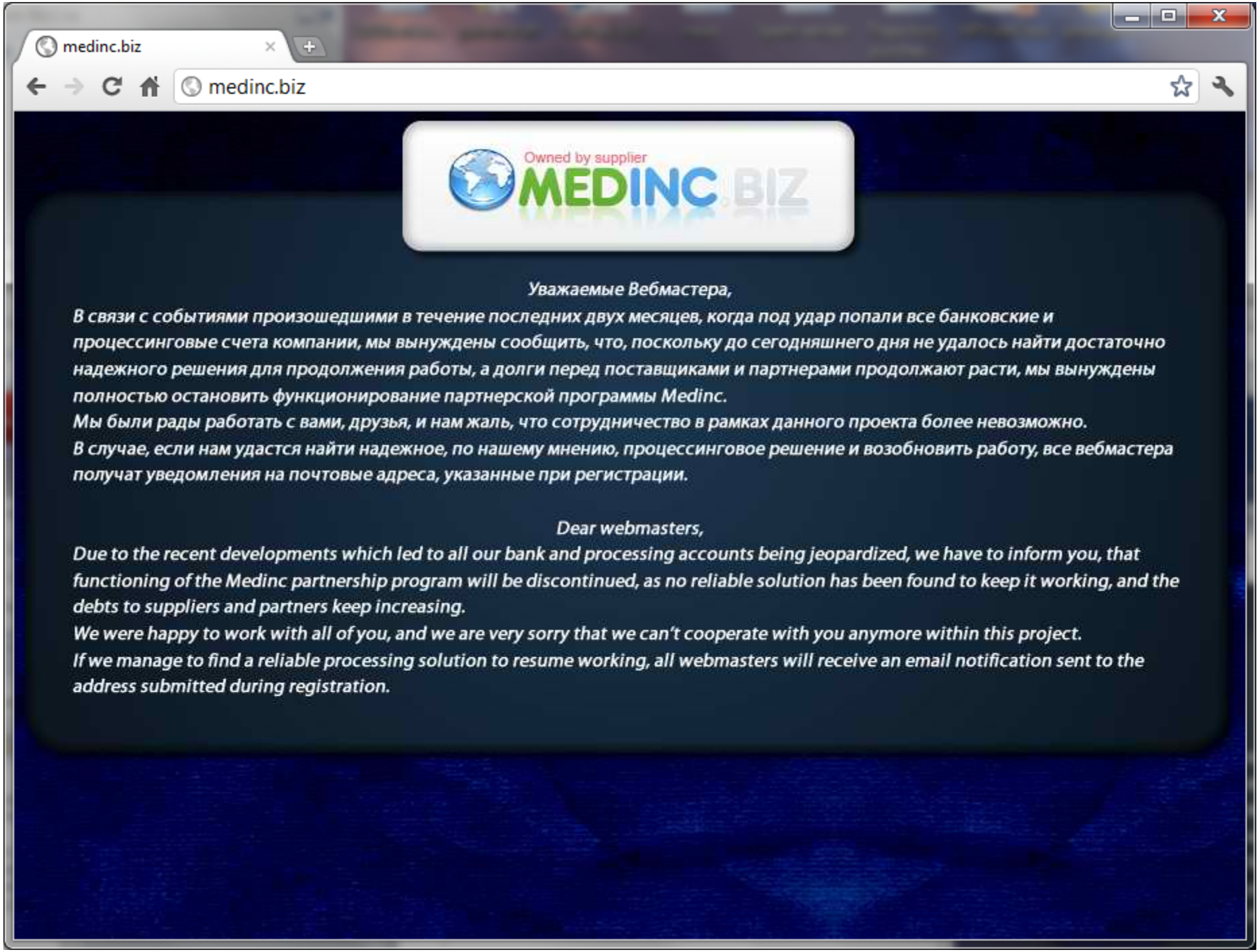
Spammers and Their Bankers

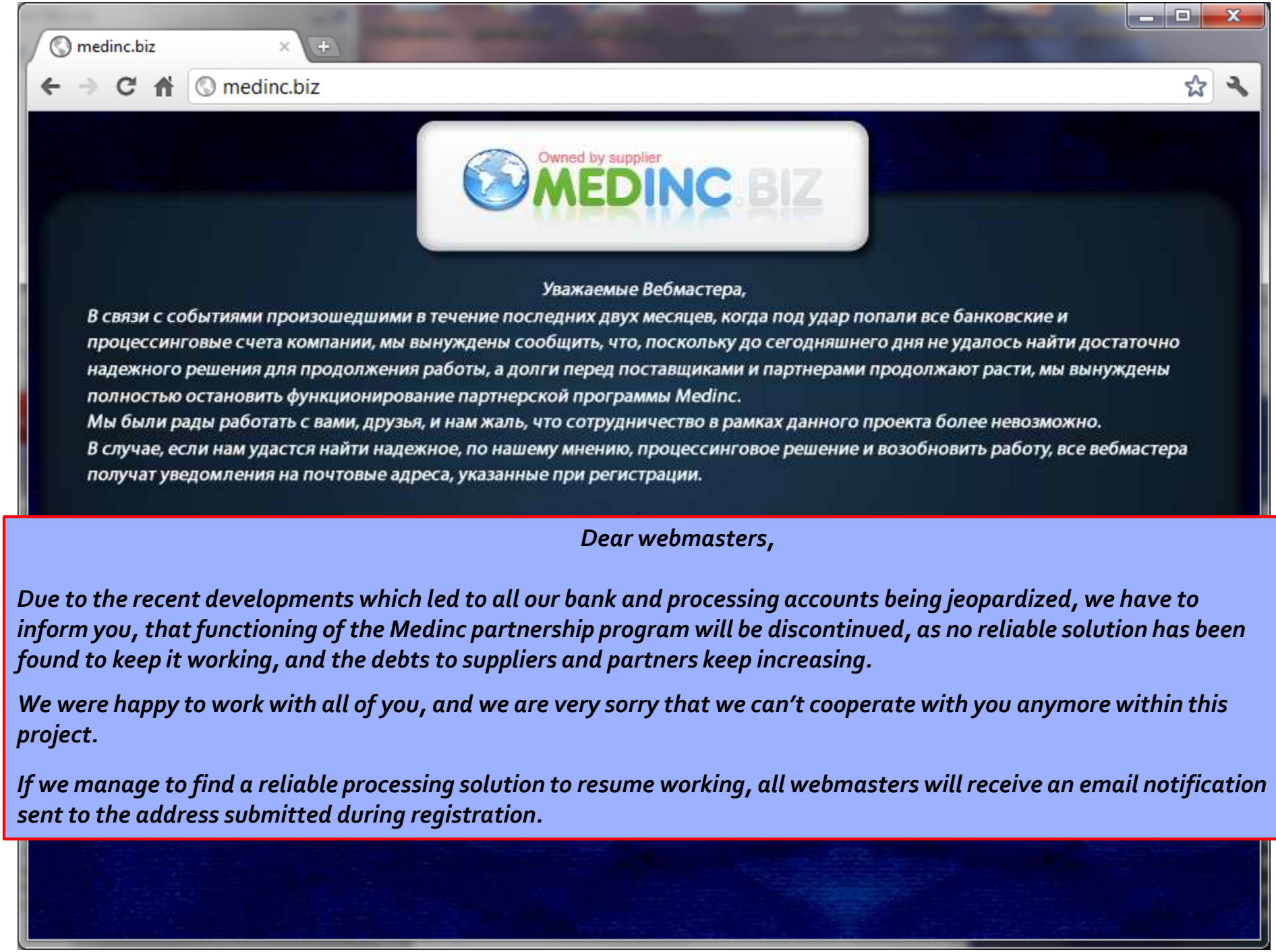
Published: May 28, 2011

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


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.

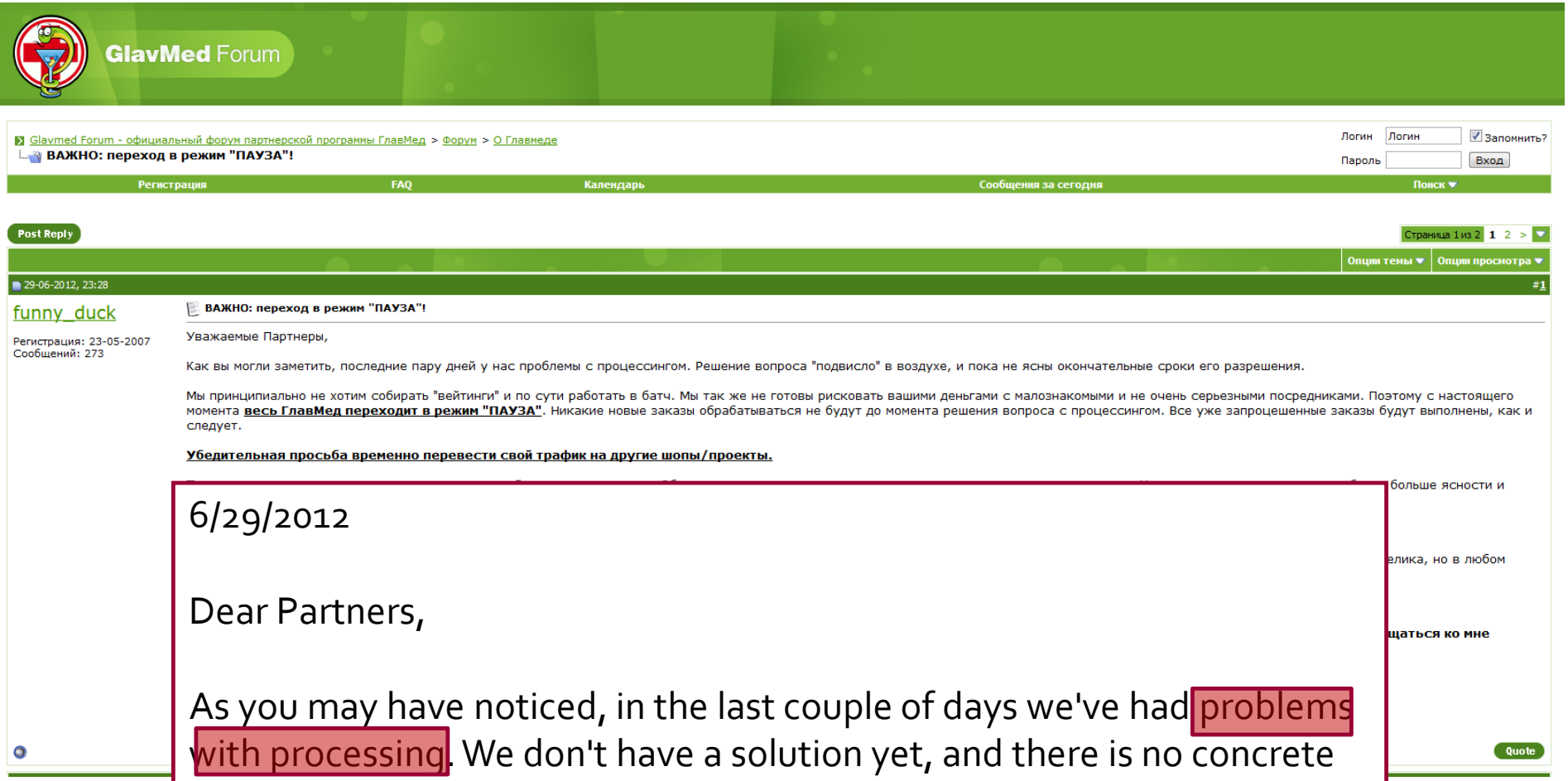


Dear webmasters,

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.



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.

.....

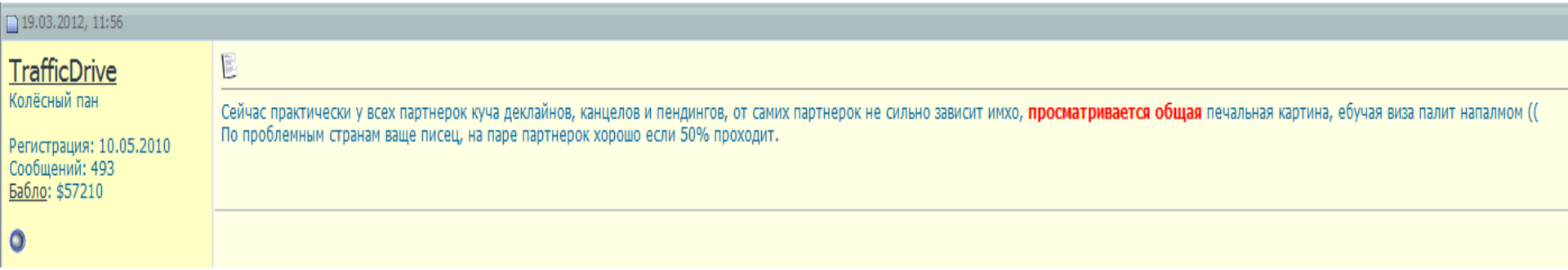
We urge you to temporarily switch your traffic to other shops/projects.

19.03.2012, 11:56

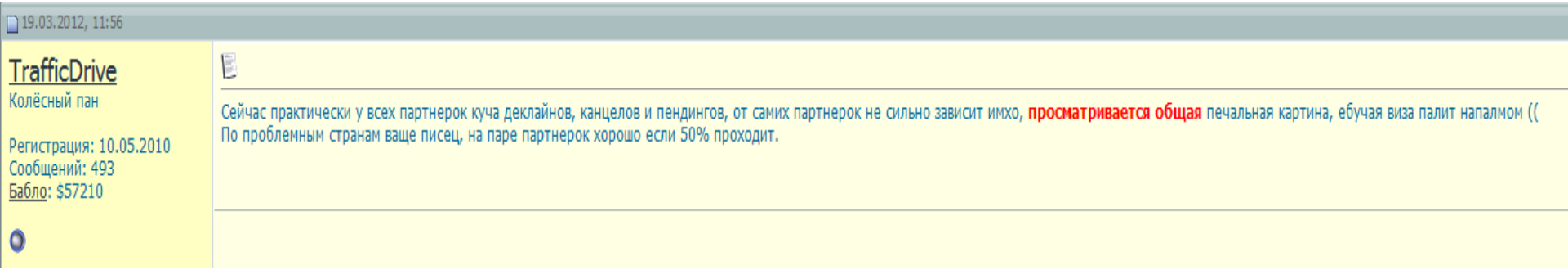
TrafficDrive
Колёсный пан

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.



"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)."



"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)."