

Buying Drugs for Science: Addressing the Economics of Cybercrime

Stefan Savage
UC San Diego

joint work w/Neha Chachra, Brandon Enright, Mark Felegyhazi (ICSI), Chris Grier (Berkeley), Tristan Halvorson, Chris Kanich, Christian Kreibich (ICSI), Kirill Levchenko, He "Lonnie" Liu, Justin Ma, Damon McCoy, Vern Paxson (ICSI/Berkeley), Andreas Pitsillidis, Geoff Voelker, and Nick Weaver (ICSI)

The traditional view of security

- Computer security is a **technical problem**
 - There are some software or design flaws
 - These flaws can be exploited by adversaries
- If we fix these technical problems then we will be secure
- But you better get them all because the adversary is adaptive...

But, today's best practices...

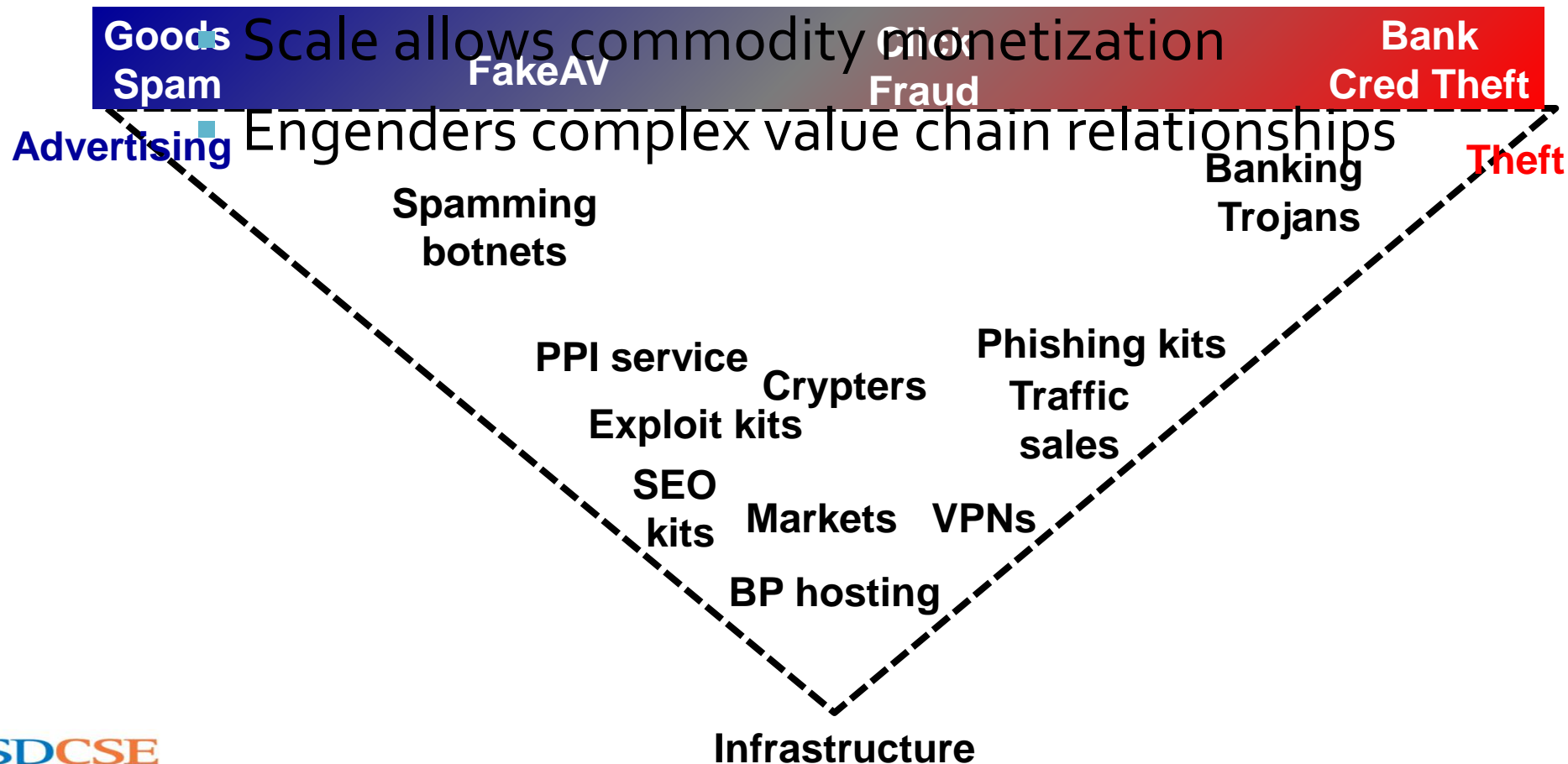


... have not stopped our adversaries

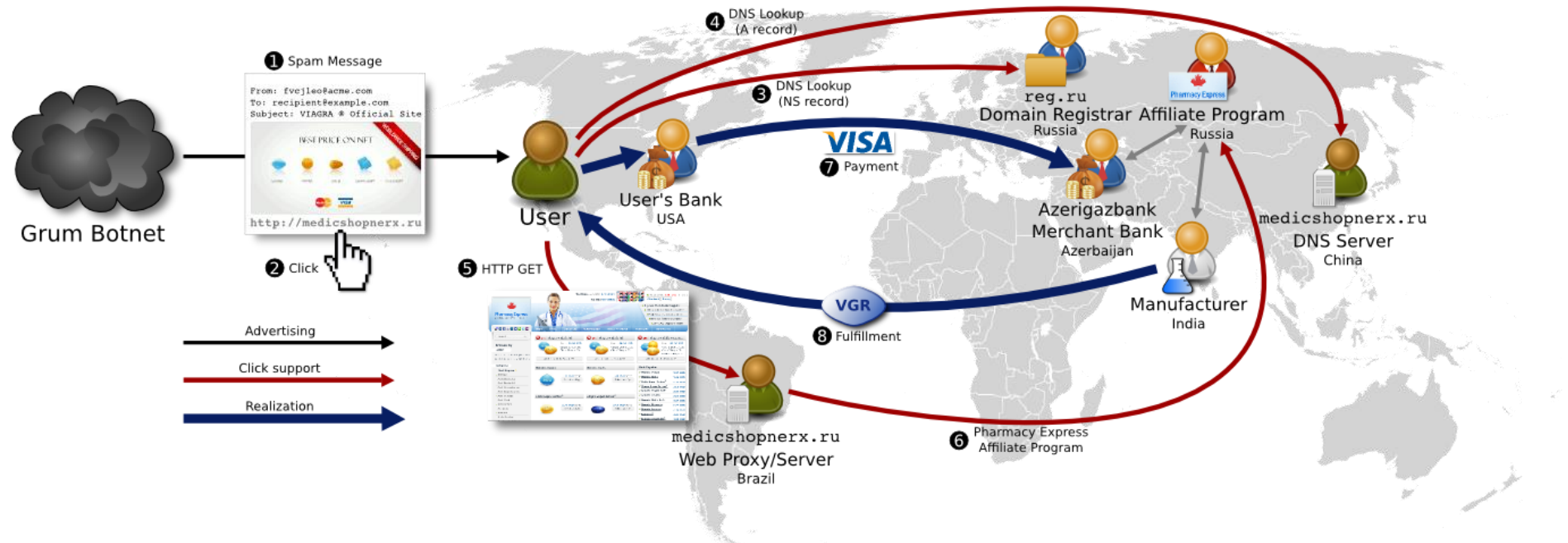


Profit driven e-crime

- The largest driver for threats is \$\$\$



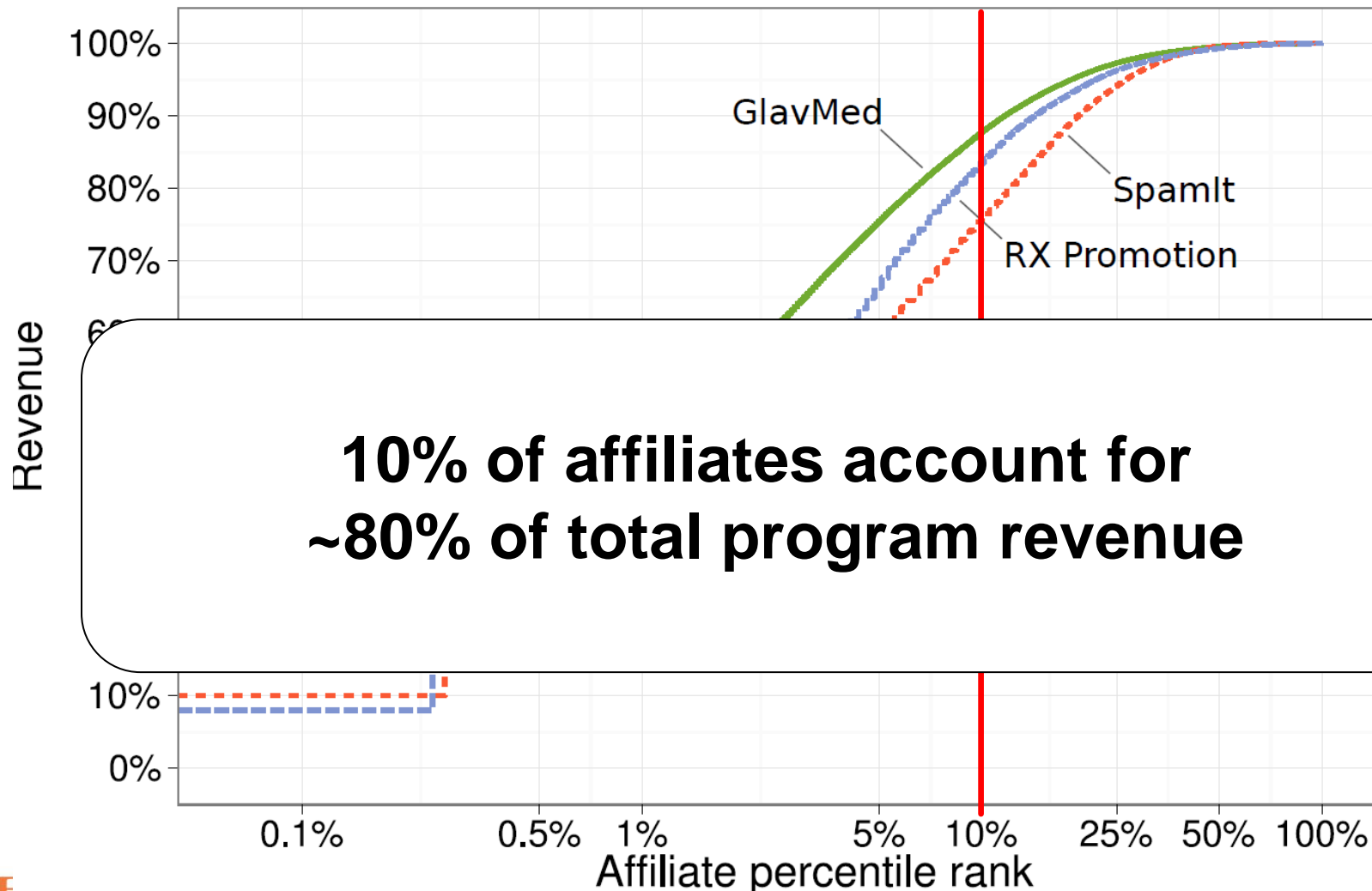
Today: the spam ecosystem



Affiliate program structure

- Division of labor
 - **Affiliates** handle advertising (e.g., spam, SEO)
 - Independent contractors
 - Paid 25-60% commission depending on kind of program
 - **Affiliate programs** handle backend
 - Payment processing, customer service, fulfillment
 - Sometimes hosting and domain registration
- Why?
 - Transfer of risk: innovation risk vs investment risk
 - Specialization lowers cost structure

Heavy-tailed revenue



Affiliate program cost structure

Example: RX-Promotion

Direct costs: 70.8%
Indirect costs: 12.8%
Profit: 16.3%

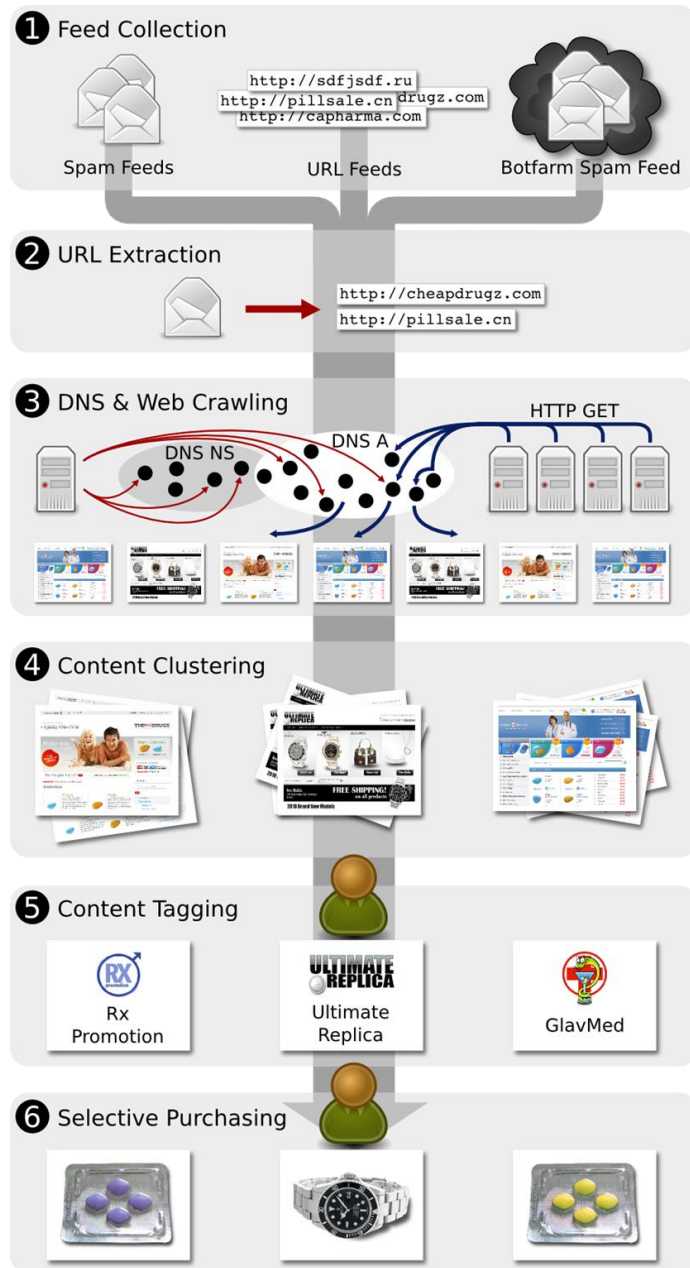
RX-Promotion
March – September 2010

Gross revenue	\$7.8M
Direct costs	\$5.5M (70.8%)
Commissions	\$3M (38.1%)
Suppliers ^a	\$1.4M (17.6%)
Processing	\$1M (13.2%)
Other direct	\$148.3K (1.9%)
Indirect costs	\$1004K (12.8%)
Administrative	\$197K (2.5%)
Customer service	\$124K (1.6%)
Fines	\$107K (1.4%)
IT expenses	\$202K (2.6%)
Domains	\$114K (1.5%)
Servers, hosting	\$66K (0.8%)
Selling expenses	\$315K (4%)
Marketing	\$105K (1.3%)
Lobbying	\$157K (2%)
Other indirect	\$134K (1.7%)
Net revenue	\$1.3M (16.3%)



Click Trajectories

- Click Trajectory project
 - Find “bottlenecks” in the spam value chain
 - Place where intervention could be most effective
 - **Resources with largest impact on profitability**
 - **Highest switching cost for adversary**
- Measure empirically
 - Resources needed to monetize each piece of spam
 - By playing the role of customer; at scale
 - Three domains: pharma, replica, software



- Click Trajectories study [Levchenko, IEEE S&P 2011]
- Aug 1 -- Oct 31 2010
- 7 URL/Spam feeds + 5 botnet feeds
 - 968M URLs, 17M domains
 - 99% of pharma, OEM, replica
- Crawled domains for 98% of URLs in
 - 1000s of Firefox instances
 - Large IP address diversity
- Hundreds of purchases
 - **Unique card # per order**
 - **Full transaction data**

Example: What if you ordered from these guys?

CANADIAN
Health&Care Mall

ALL PRODUCTS | ABOUT US | HOW TO ORDER | TESTIMONIALS | FAQ | CONTACTS

Bank Identification Number (BIN) 448314



Merchant descriptor "Smart rt online"

Card Acceptor ID "8875236"

Merchant Category Code (MCC) 5912

Drug Stores & Pharmacies



Director of purchasing

Project lead



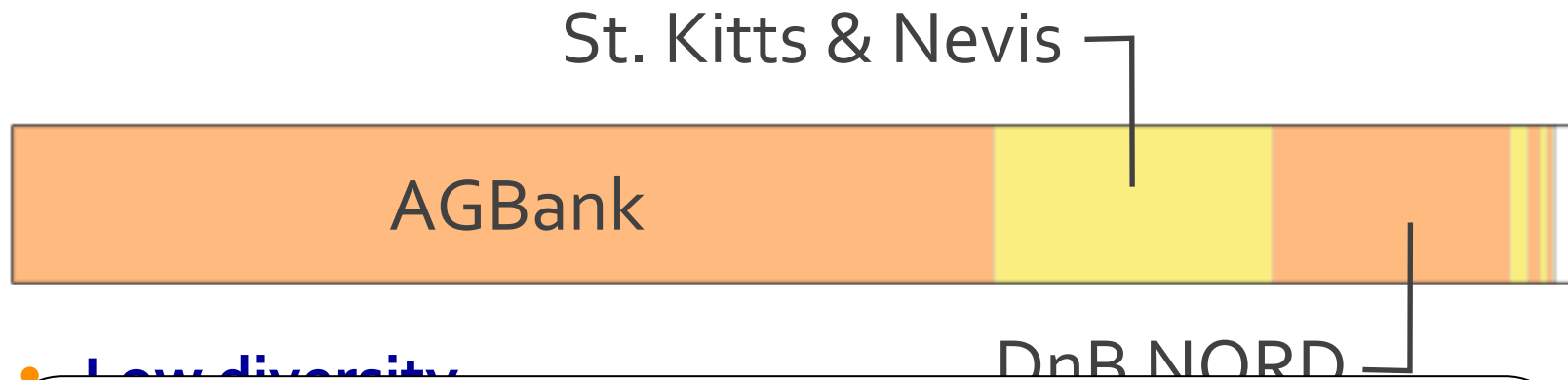
600+ orders later...



The big finding

- Most resources are cheap and plentiful
- Replacement cost < expected profit
 - This is why shutting down domains and Web sites is unlikely to ever work
- One major exception...

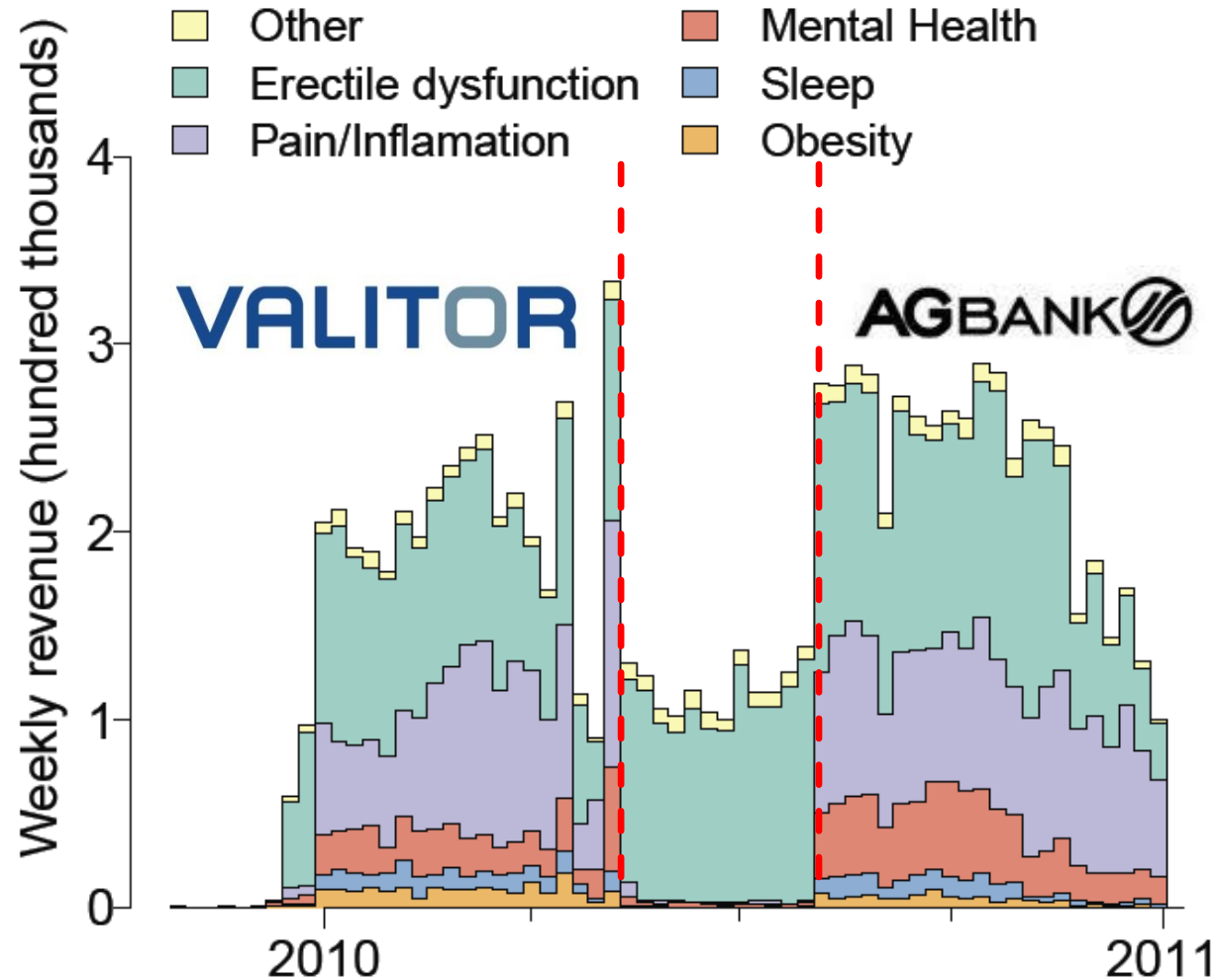
Merchant banks (circa late '10)



Hypothesis: Targeting merchant accounts could have major impact

- Money: Upfront capital, holdback forfeiture (big deal)

Anecdotal evidence: Revenue by drug type (RX-Promo)



Nice academic result, but so what?

- A stew of activities
 - Encouragement from D.C.
 - Brand interest
 - Card association cooperation
 - Complex politics around SOPA/PIPA/etc
- Two major changes
 - Visa Global Brand Protection Program (GBPP)
 - Targeted merchant intervention (IACC & brands)



Targeted payment intervention today

- **Undercover** test purchase at counterfeit site
 - Get merchant bank BIN from transaction
- IP holder notifies card network (e.g., Visa/MC)
 - Investigation; complaint delivered to merchant bank
- **Leverage via card association contract**
 - Merchant bank owns liability
 - Fines, increased scrutiny, de-association
- Merchant account shutdown

So... does it work?

- Bottom line: **Yes, amazingly well.**
- We've tracked bank association w/affiliate programs for almost two years (continuing...)
 - ~1000 purchases (Visa only)
- Joined programs as affiliates to get damage assessment from inside
- Quick stories: OEM software and Pharma

Major OEM affiliates



По вопросам регистрации и супорта обращаемся смело @ 371-777

OEMCash

SOFT MÖNSTER

ПРИВАТНАЯ OEM-ПАРТНЕРКА – СИЛА!
БОЛЬШОЙ ВЫХОД!



WAREZSTORE.COM



software sellers



OEM Soft Store
Easy and Fast Download

OEM 2012

Affiliate Login

Email

[Forgot Password?](#) [Sign Up Now](#)

Autodesk Adobe Microsoft symantec COREL

SUPPORT 4255909 support@oempartners.biz

DEM EMPIRE
OEM ПАРТНЕРСКАЯ ПРОГРАММА
НАЦИОНАЛЬНЫЙ ЦЕНТР ЗАЩИТЫ ИНТЕРЕСОВ ПОЛЬЗОВАТЕЛЕЙ

Система Партнерства, Регистр, Статистика
Настройка: 02.04.2010, 16:00
Заработок за все время: 2330.79
Привлечено: 103/127
Продажи: 10/17

Общая статистика

Кликнул по баннеру (по Sub-Account (по реферру (по GEO IP (по реферру (по периоду

Период	Кликнул по баннеру	Sub-Account	реферру	GEO IP	реферру	периоду	Минус
15/04/2010	0	0	0	0	0	0	0.00
17/04/2010	0	0	0	0	0	0	0.00
18/04/2010	0	0	0	0	0	0	0.00
19/04/2010	0	0	0	0	0	0	0.00
20/04/2010	460	1224	0	2120	1230	46.83	21.94
21/04/2010	413	2063	0	1120	1413	399.76	36.88
22/04/2010	833	2038	0	2103	1417	181.68	134.68
23/04/2010	460	1224	0	2120	1230	46.83	21.94
24/04/2010	1270	2070	0	2103	1424	84.83	101.76
24/04/2010	1280	2078	0	2103	1426	185.75	145.46
25/04/2010	1827	3630	0	8100	1283	187.00	159.92
26/04/2010	1280	2070	0	2103	1424	84.83	101.76
27/04/2010	0	0	0	0	0	0	0.00
28/04/2010	0	0	0	0	0	0	0.00
29/04/2010	0	0	0	0	0	0	0.00
30/04/2010	0	0	0	0	0	0	0.00
Итого	7483	14868	0	38123	8266	147.33	1167.27

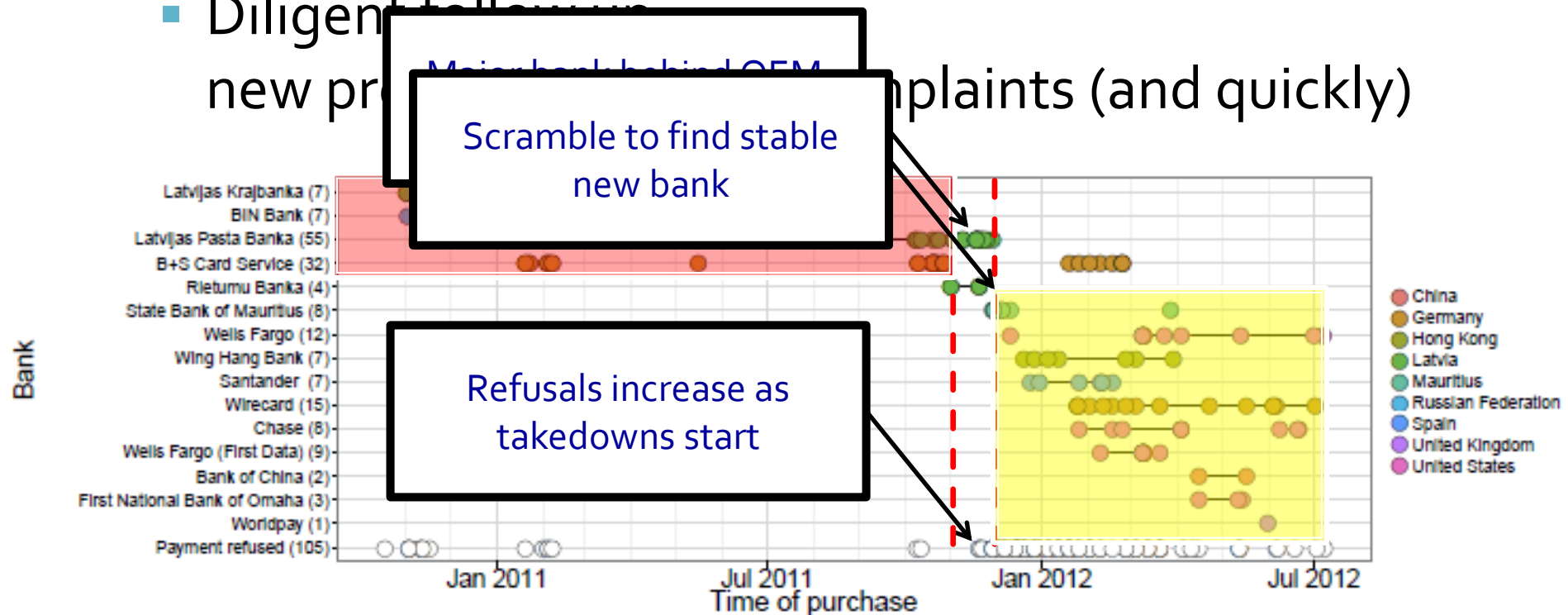
Главная | Статистика | Настройка | Пресс | Реклама | Контакты
© 2010 Dem Empire
All Rights Reserved



UCSD CSE
Computer Science and Engineering


OEM software story

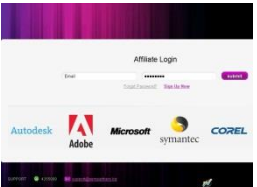
- Microsoft's Thanksgiving present (Nov '11)
 - Methodically issued complaints for accounts of **every** major affiliate program
 - Diligent follow-up on new programs (and quickly)



Qualitative Timeline

11/2011: Microsoft starts merchant complaint actions

11/20/2011: ATTENTION! Деяка з наших партнерів, які мали великі банківські проблеми, банком заблокували результати. Ми були змушені тимчасово зупинити всі банківські трафіки. 

2011-11-22 10:16:38 Старт роботи однієї з наших банків. Due to this, we have a (problem) in this system affiliate program for the activation of our affiliate program. 

1/23/2012 Remark by leading affiliate:
"The sun is setting on the OEM era"



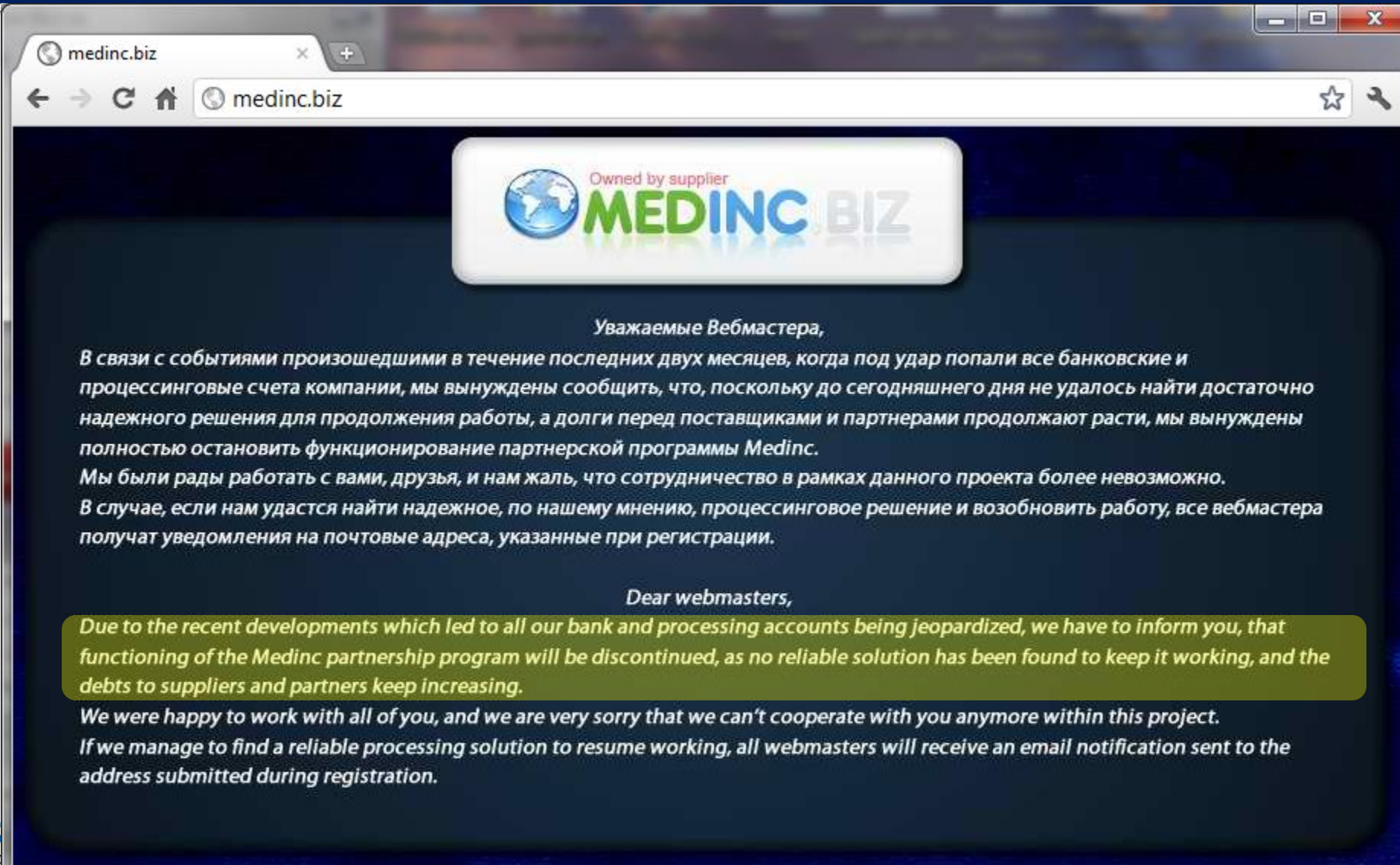
Today

- OEM software market has been **decimated**
 - 90% of programs have folded
 - New startups (softbuy) shut down quickly
- Affiliates still operating won't sell Microsoft software

The pharma story

- Much more developed ecosystem
- Intervention less focused, less comprehensive, less follow up
- Still significant impact...

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.

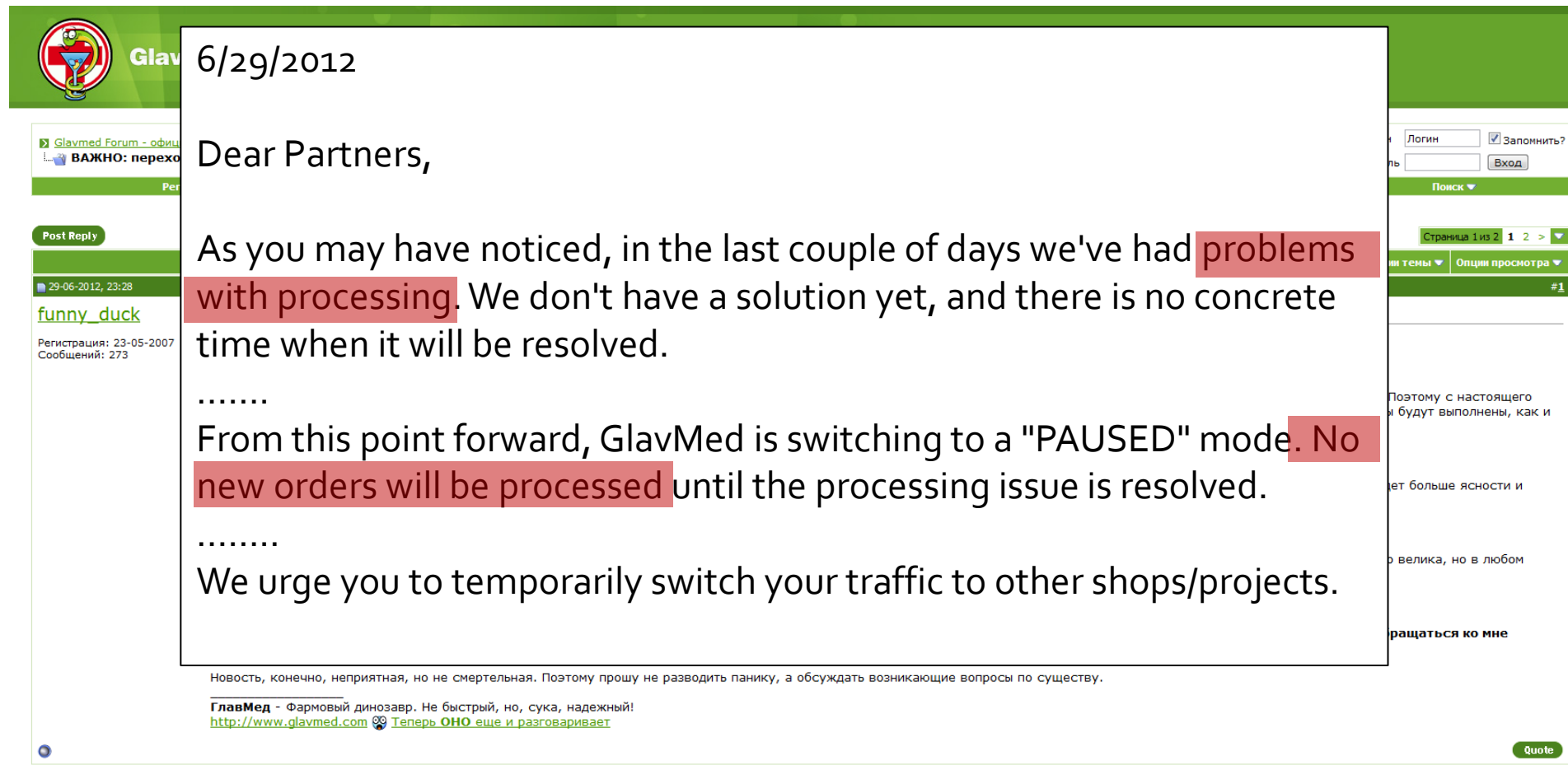
Dear webmasters,

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.

Glavmed



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.

Новость, конечно, неприятная, но не смертельная. Поэтому прошу не разводить панику, а обсуждать возникающие вопросы по существу.

ГлавМед - Фармовый динозавр. Не быстрый, но, сука, надежный!
<http://www.glavmed.com>  [Теперь ОНО еще и разговаривает](#)

Quote



OxoPharm

27.06.2012, 17:41 #104

DaoVlad
DaoNetwork
Регистрация: 17.02.2009
Сообщений: 118
Балло: \$30743

from Sipler
Всем привет!

Хочу сообщить адвертам партнерки OXOnetwork, что мною было принято решение о ее закрытии. Уже официально. Чтобы не было глупых домыслов, считаю нужным объяснить причину.

Главная Партнерка закрывается не из-за финансовых проблем. Тут ничего говорить даже проект достаточно прибыльный

Бо

ик на другую

одскажет, что

нерки, к

Hello all!

I would like to notify the advertisers of the OXOnetwork affiliate program that I have made the decision about its closure.

...

Если у вас есть еще какие-то вопросы, то стучите в саппорт, все будем решать.
Всем спасибо за работу.

Удачи! 🍀

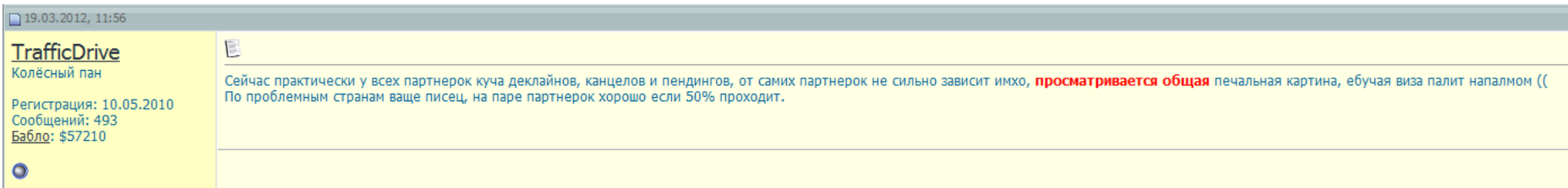
P.S. Я никак не могу восстановить пасс для GFB, поэтому этот текст запостит саппорт.

Cashadmin



- To all Cashadmin affiliates,
RX industry is under attack from all sides. Recently, we have lost our credit card processing abilities several times, and it has come to the point where we are losing more money processing orders than we are getting from the orders themselves. The industry has become impossible to manage and maintain. Cashadmin has closed its sites...

Life is tough all around...



“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).”

Pharma programs accepting US Visa purchases in 2011



Stimul Cash
JUST WHAT THE DOCTOR ORDERED



Pharma programs accepting US Visa purchases today



Summary

- Our research is driven by two beliefs
 - Effective intervention will require reasoning about the economic/social structure of our adversaries
 - This reasoning should be informed by empirical measurement data and fieldwork
- This research agenda is both **achievable** and has the opportunity for major **impact** (both for research and the real world)

Questions?

