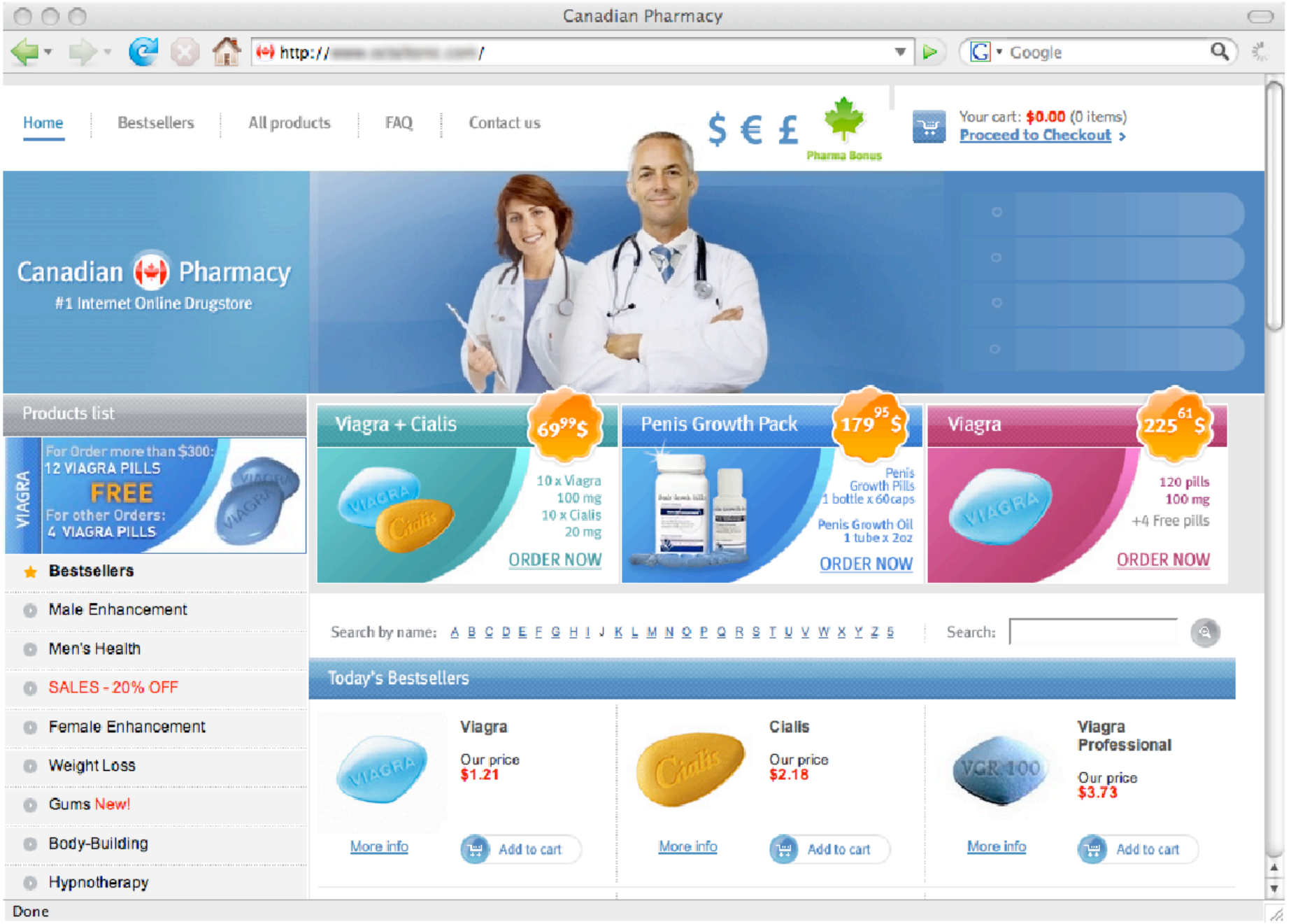
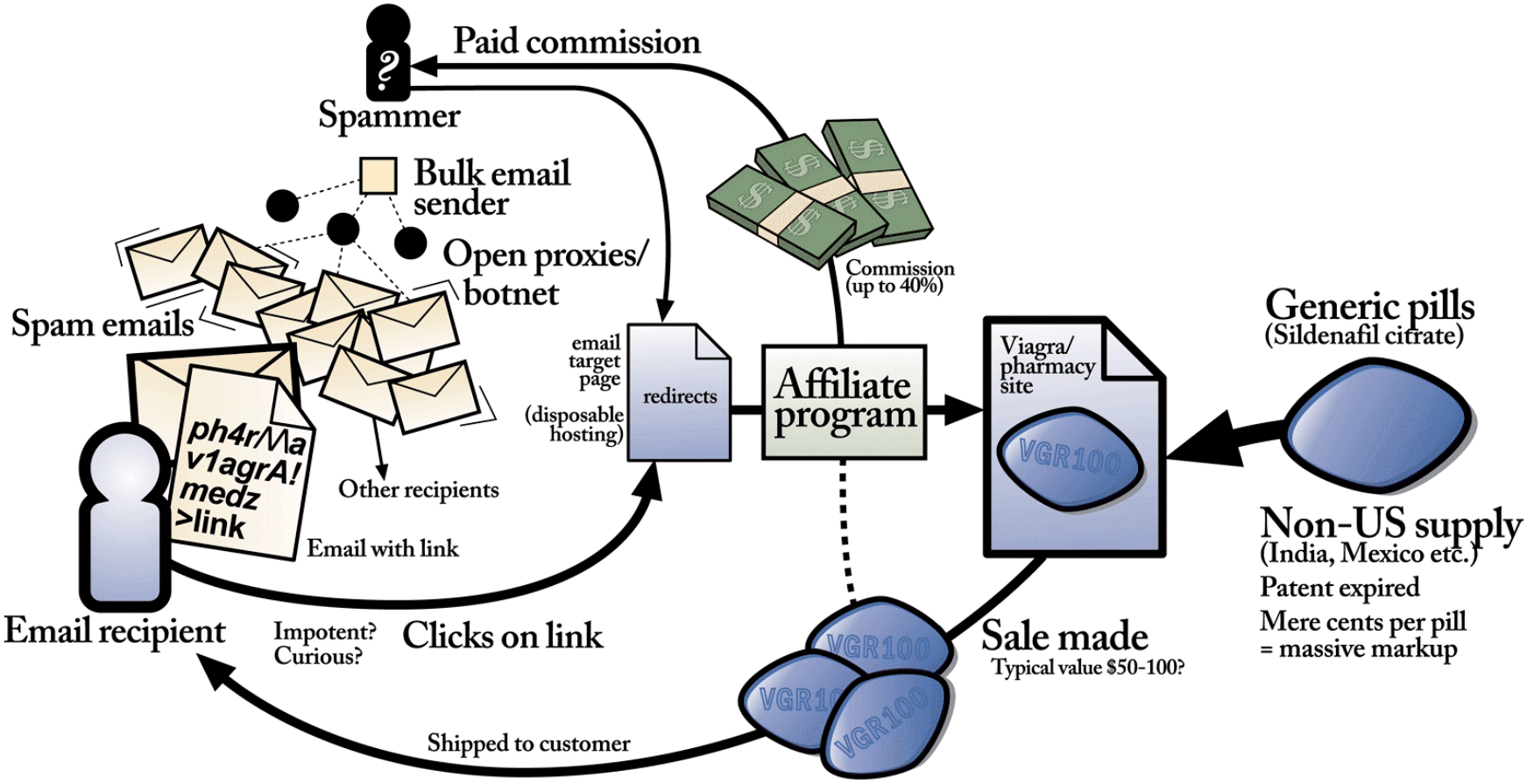

Canadian Pharmacy
http://
Google
Home
Bestsellers
All products
FAQ
Contact us
$ € £
Pharma Bonus
Your cart: $0.00 (0 items)
Proceed to Checkout
Canadian Pharmacy
#1 Internet Online Drugstore
Products list
VIAGRA
For Order more than $300:
12 VIAGRA PILLS
FREE
For other Orders:
4 VIAGRA PILLS
Bestsellers
Male Enhancement
Men's Health
SALES - 20% OFF
Female Enhancement
Weight Loss
Gums New!
Body-Building
Hypnotherapy
Viagra + Cialis
69.99$
10 x Viagra
100 mg
10 x Cialis
20 mg
ORDER NOW
Penis Growth Pack
179.95$
Penis Growth Pills
1 bottle x 60caps
Penis 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

Anatomy of a modern Pharma spam campaign



Courtesy Stuart Brown
modernlifeisrubbish.co.uk

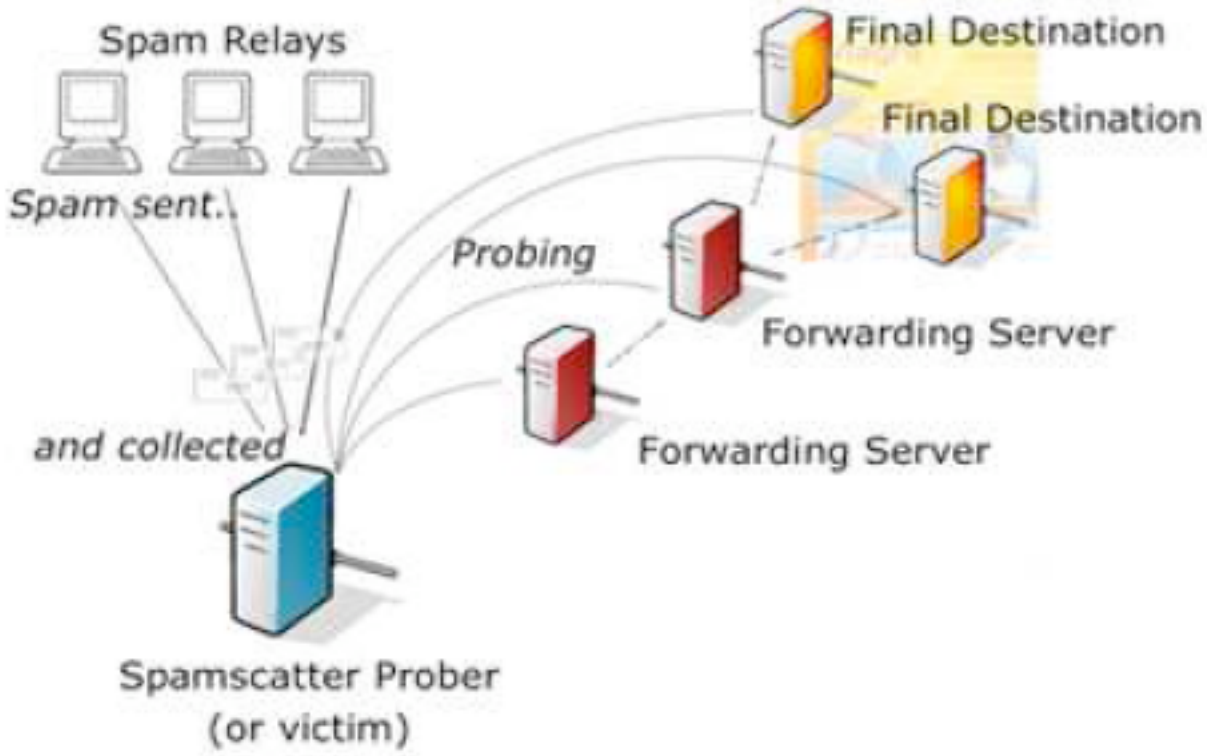
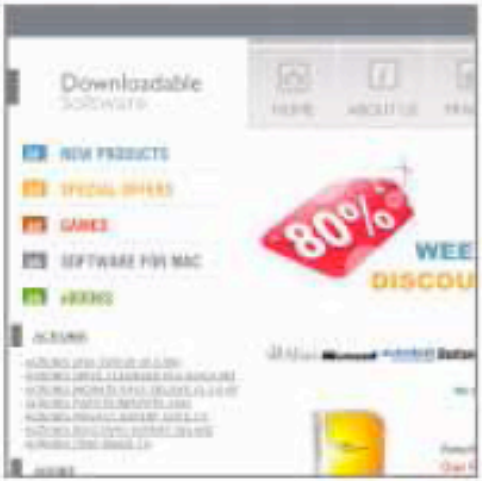
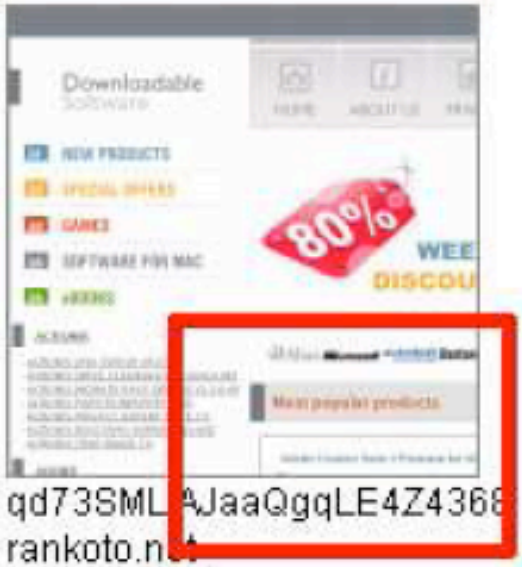


Figure 1: Components of a typical Internet scam.



hDOcrKgDajD0GxuBJpz10330
gubi-soft.com
193.124.8.218



qd73SML AJaaQgqLE4Z4368
rankoto.net
221.4.246.3

6n9JvOkPZTkuwPEnYzH3918
gro.uronila-soft.com
193.124.8.218

cMCicUSGT2rE7dd2Sy92829
ne.gubi-soft.net
193.124.8.218

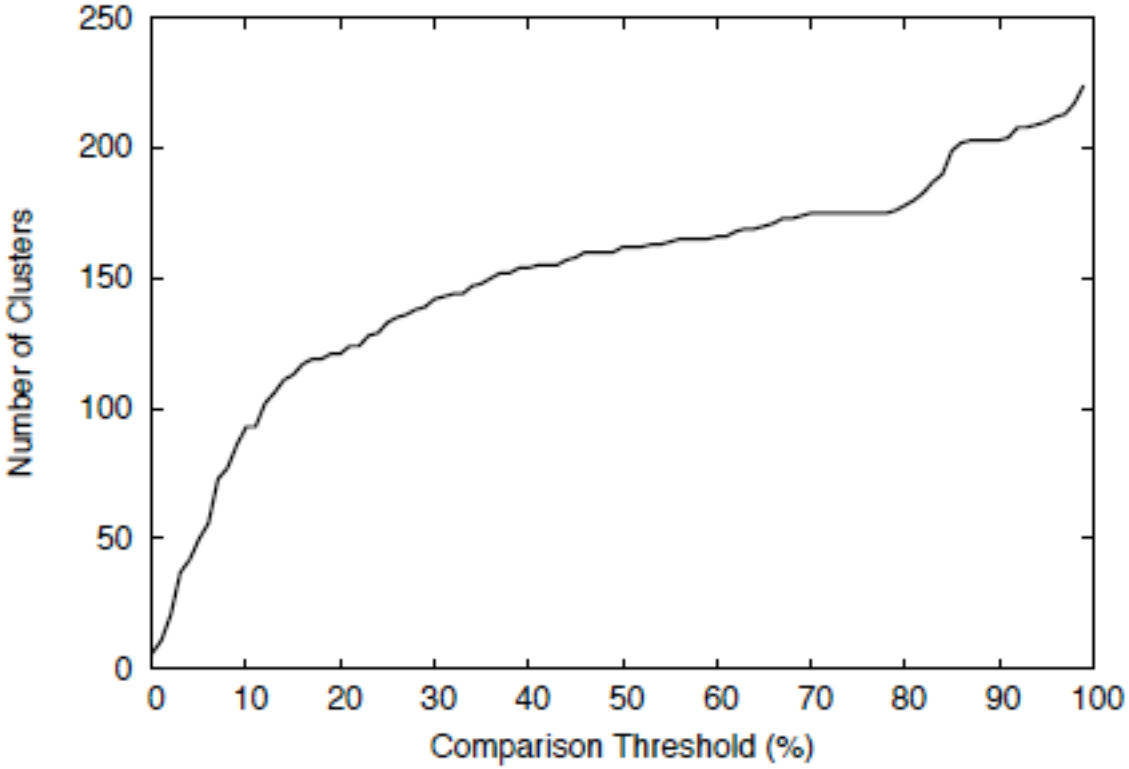


Figure 4: The choice of a threshold value for image shingling determines the number of clusters.

Characteristic	*Summary Result*
Trace period	11/28/06 – 12/11/06
Spam messages	1,087,711
Spam w/ URLs	319,700 (30% of all spam)
Unique URLs	36,390 (11% of all URLs)
Unique IP addresses	7,029 (19% of unique URLs)
Unique scams	2,334 (6% of unique URLs)

Table 1: Summary of spamscatter trace.

Scam category	*% of scams*
Uncategorized	29.57%
Information Technology	16.67%
Dynamic Content	11.52%
Business and Economy	6.23%
Shopping	4.30%
Financial Data and Services	3.61%
Illegal or Questionable	2.15%
Adult	1.80%
Message Boards and Clubs	1.80%
Web Hosting	1.63%

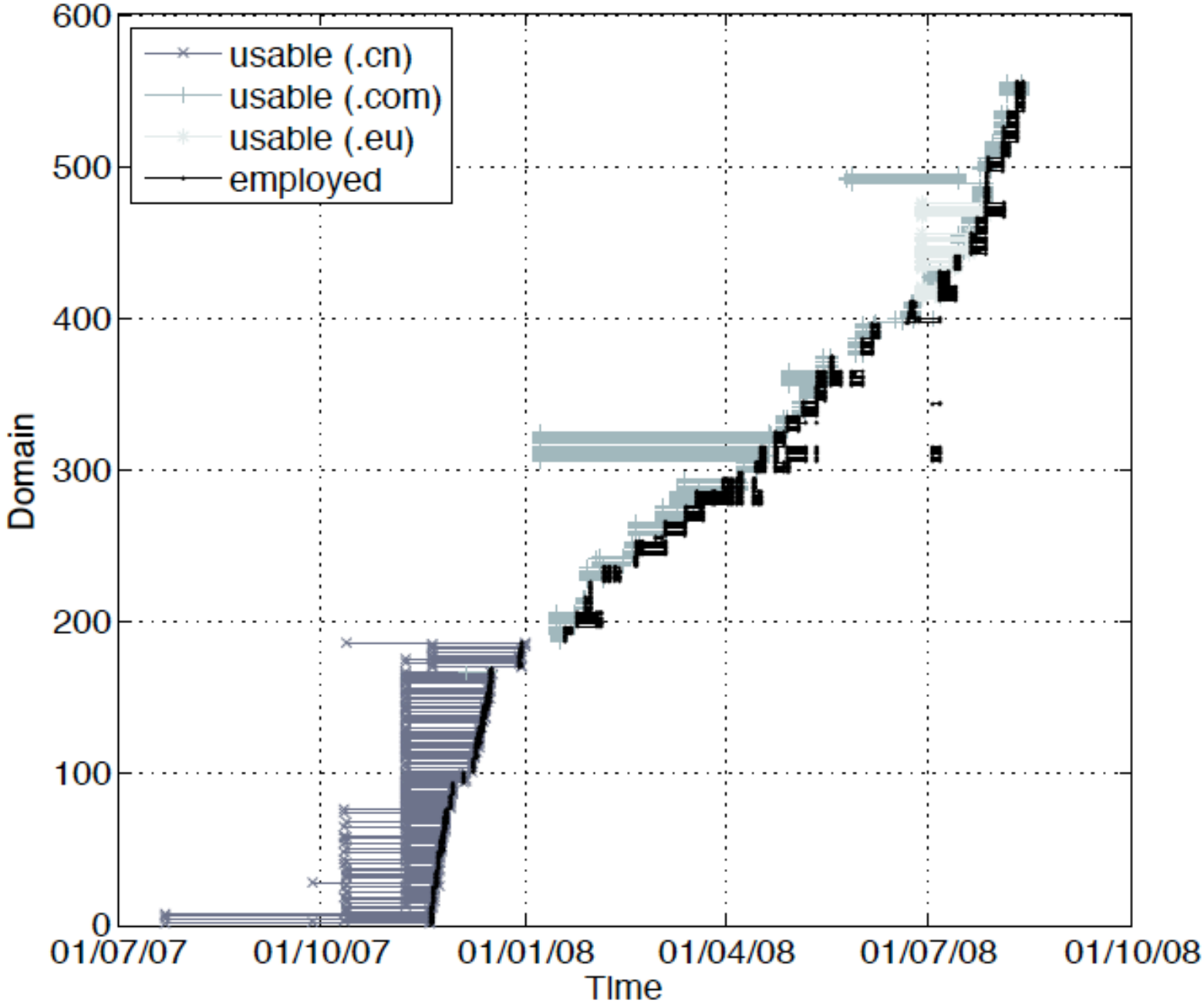
Table 2: Top ten scam categories.

Table 5. Proportion of Websites Still Alive After 6 and 4 Weeks Respectively

-	Sites > 6 weeks	Sites > 4 weeks	Sites
Child sexual abuse images	20.0%	38.0%	1400
Rock-phish domains	0.0%	0.0%	33
Fast-flux phishing	10.5%	15.7%	38
Ordinary phishing	24.0%	24.0%	25
All phishing combined	10.4%	12.5%	96

Table 2. Phishing Website Lifetimes by Attack Type

-	Sites	Lifetime (hours)	
		Mean	median
Free web-hosting			
all	395	47.6	0
brand owner aware	240	4.3	0
brand owner missed	155	114.7	29
Compromised machines			
all	193	49.2	0
brand owner aware	105	3.5	0
brand owner missed	155	103.8	10
Rock-phish domains	821	70.3	33
Fast-flux domains	314	96.1	25.5


usable (.cn)
usable (.com)
usable (.eu)
employed
Domain
600
500
400
300
200
100
0
01/07/07
01/10/07
01/01/08
01/04/08
01/07/08
01/10/08
Time

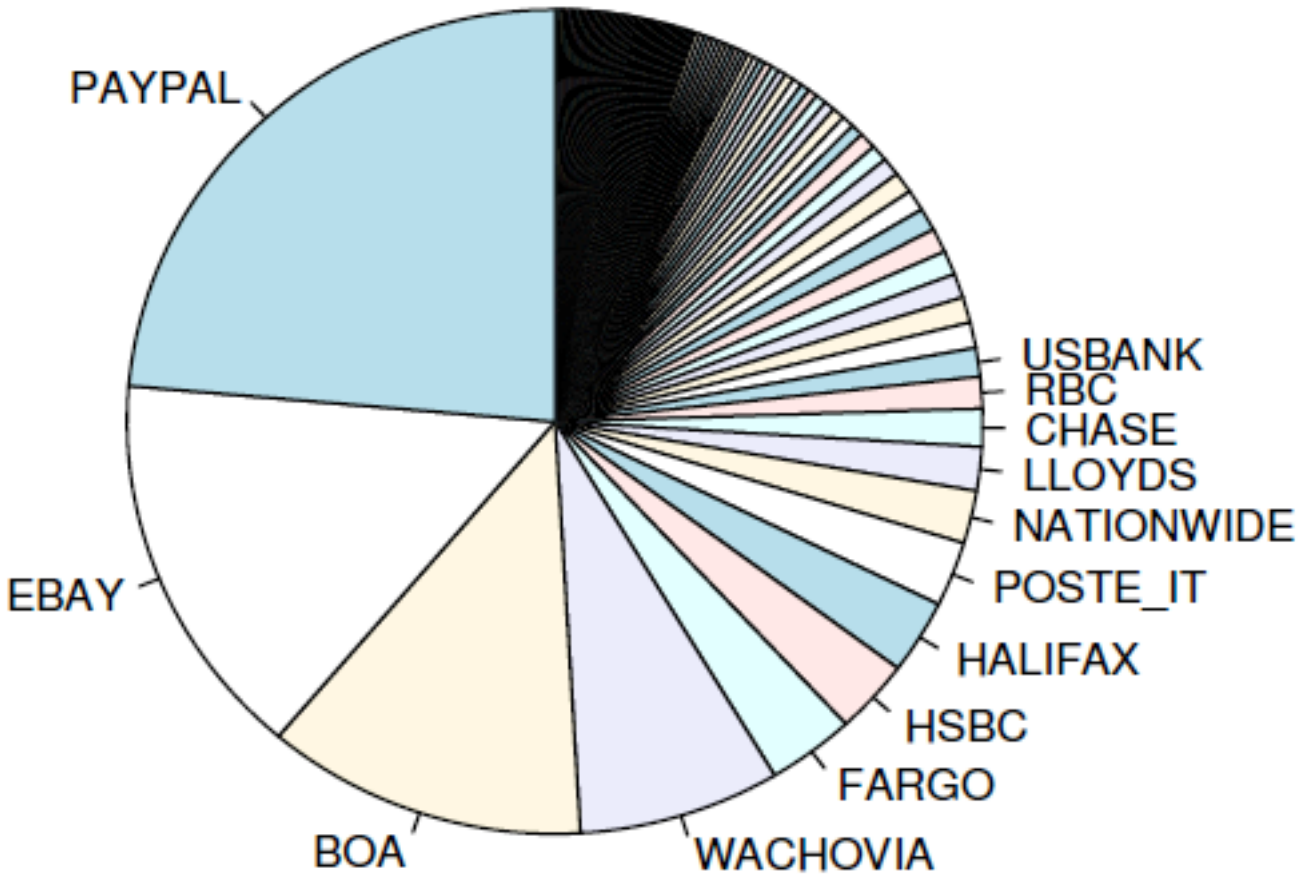


Figure 7: Proportion of ordinary phishing sites impersonating each bank.

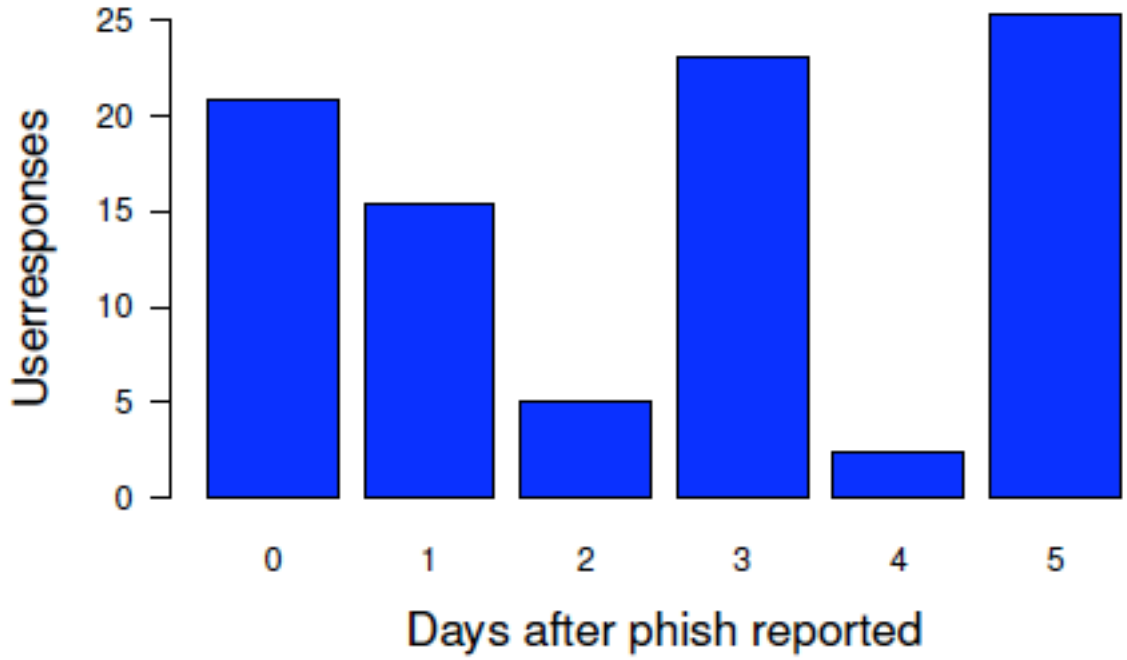


Figure 5: User responses to phishing sites over time. Data includes specious responses.

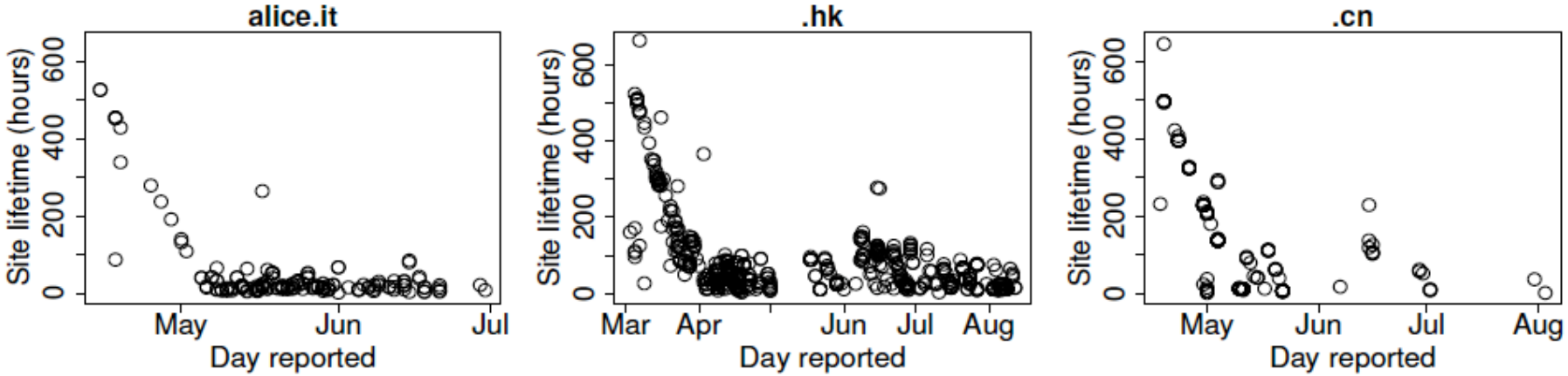


Figure 9: Scatter plot of phishing site lifetimes over time.

Are Bots & Spam the New Black Gold?

Storm worm 'making millions a day'

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

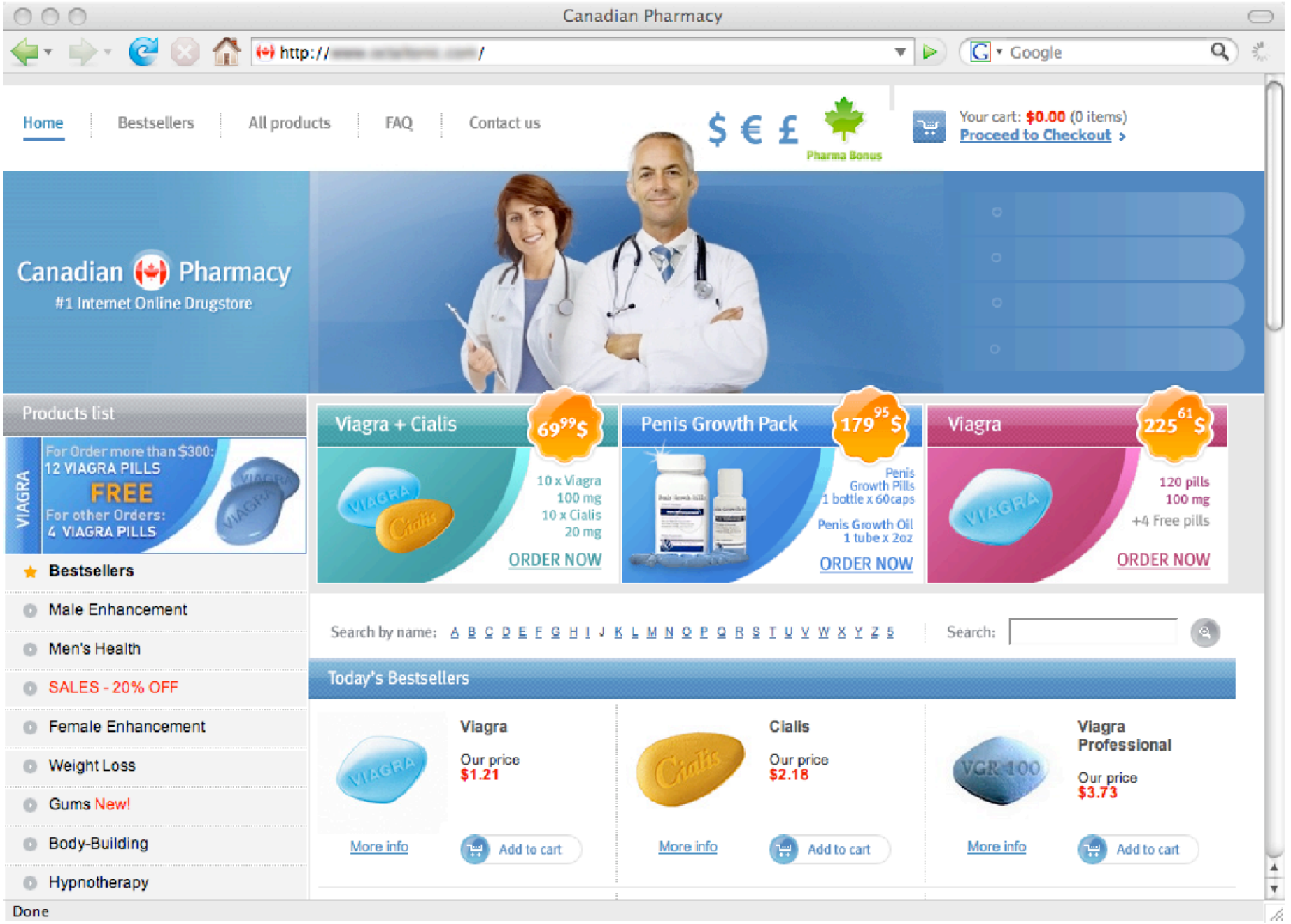
Clive Akass, Personal Computer World 11 Feb 2008

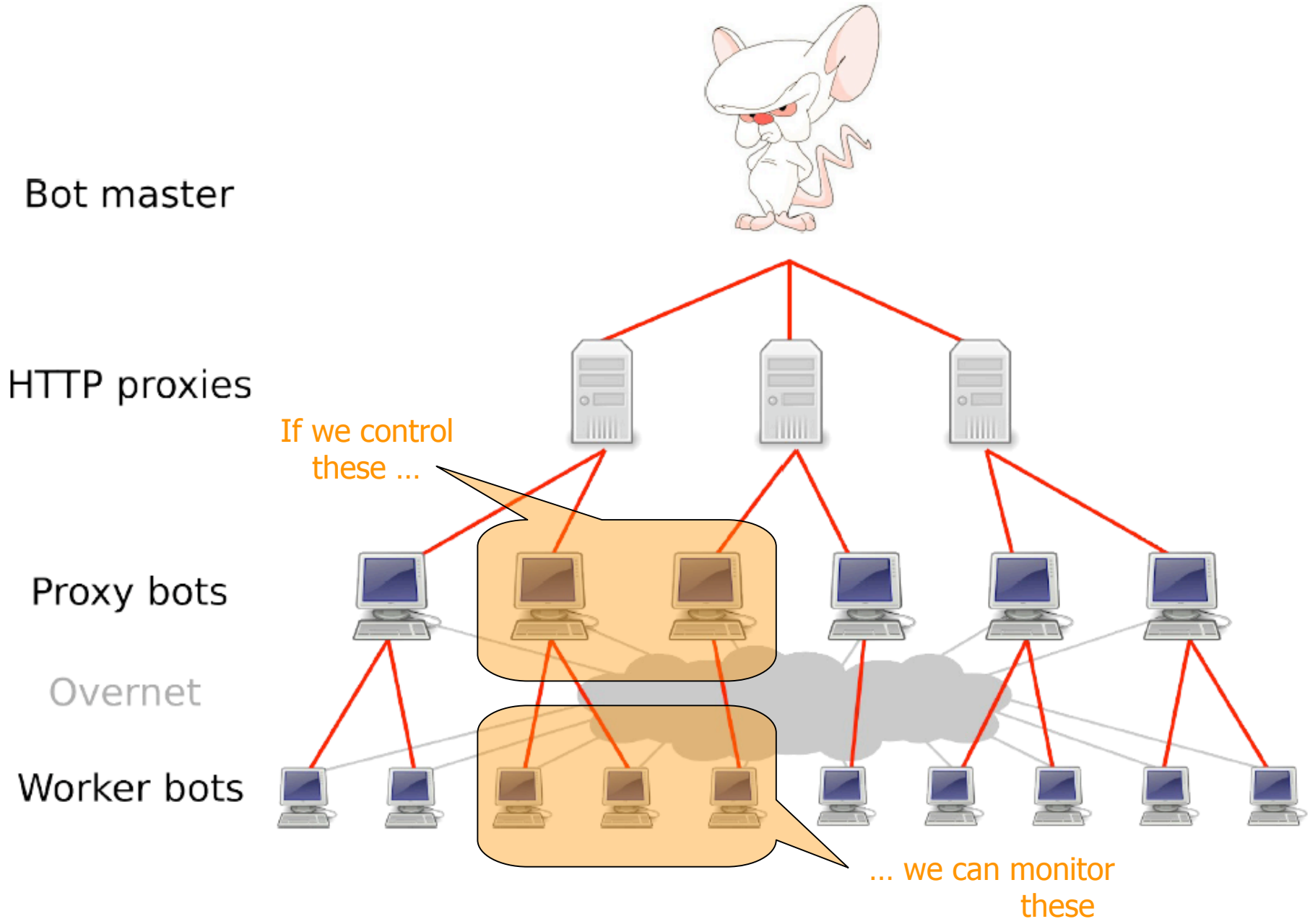
The people behind the Storm worm are making millions of pounds a day by using it to generate revenue, according to IBM's principal web security strategist.

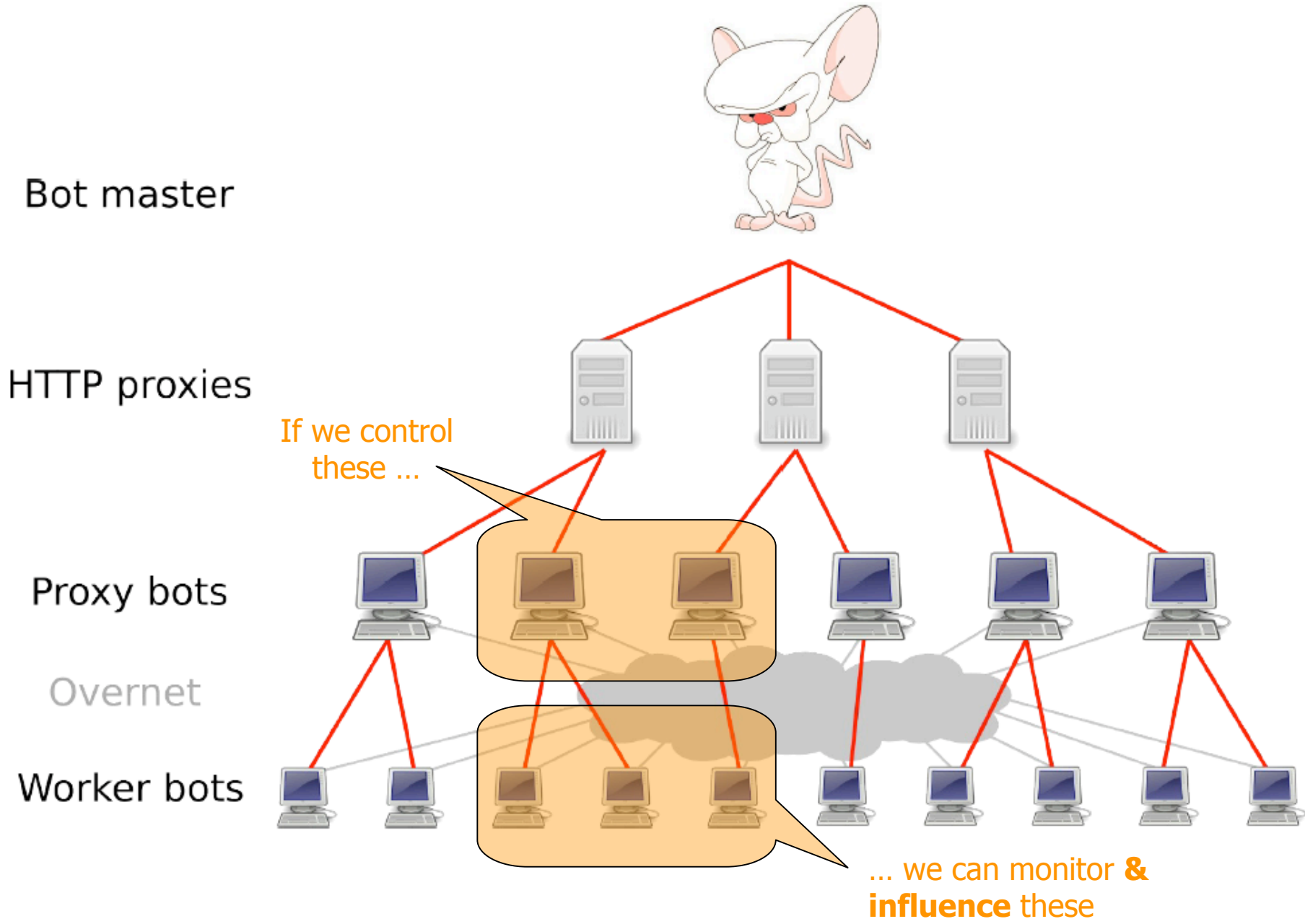
Joshua Corman, of **IBM Internet Security Systems**, said that in the past it had been assumed that web security attacks were essential ego driven.

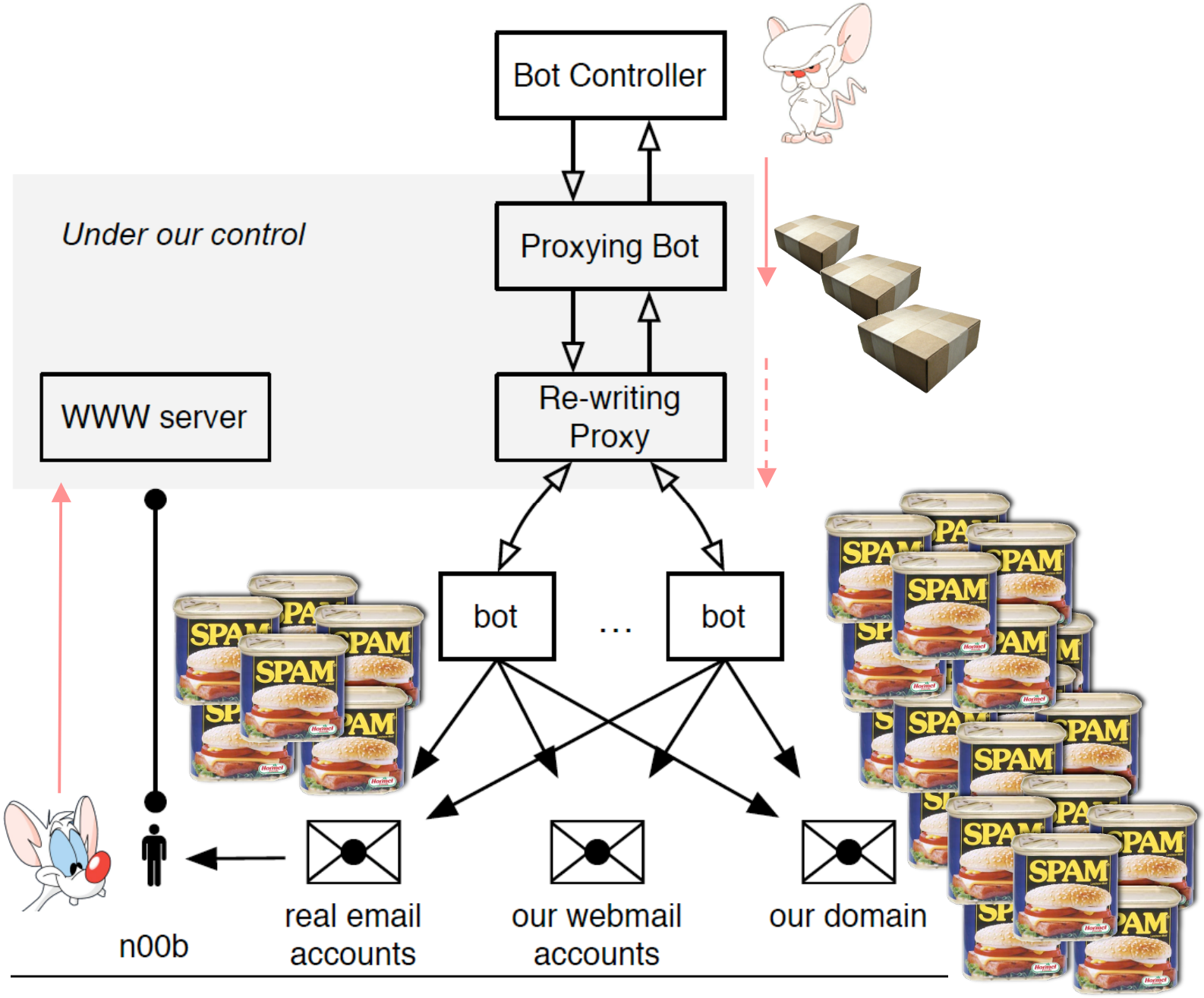
How can we **measure** this? Seemingly only knowable by the spammers themselves.

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


Canadian Pharmacy
http://
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
VIAGRA
For Order more than $300:
12 VIAGRA PILLS
FREE
For other Orders:
4 VIAGRA PILLS
Bestsellers
Male Enhancement
Men's Health
SALES - 20% OFF
Female Enhancement
Weight Loss
Gums New!
Body-Building
Hypnotherapy
Viagra + Cialis
69.99$
10 x Viagra
100 mg
10 x Cialis
20 mg
ORDER NOW
Penis Growth Pack
179.95$
Penis Growth Pills
1 bottle x 60caps
Penis 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


Bot master
HTTP proxies
If we control these ...
Proxy bots
Overnet
Worker bots
... we can monitor these


Bot master
HTTP proxies
If we control these …
Proxy bots
Overnet
Worker bots
… we can monitor & influence these

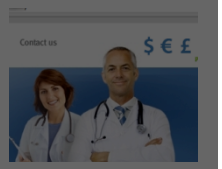

Bot Controller
Under our control
Proxying Bot
WWW server
Re-writing Proxy
bot
…
bot
SPAM
n00b
real email accounts
our webmail accounts
our domain

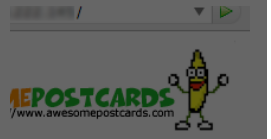
Spam conversion experiment

- Experimented with Storm March 21 – April 15, 2008
- Instrumented roughly 1.5% of Storm's total output

	Pharmacy Campaign	**E-card Campaigns**	
		Postcard	April Fool
Worker bots	31,348	17,639	3,678
Emails	347,590,389	83,665,479	38,651,124
Duration	19 days	7 days	3 days

Spa





load will start in 5 seconds.
oad does not start, click here

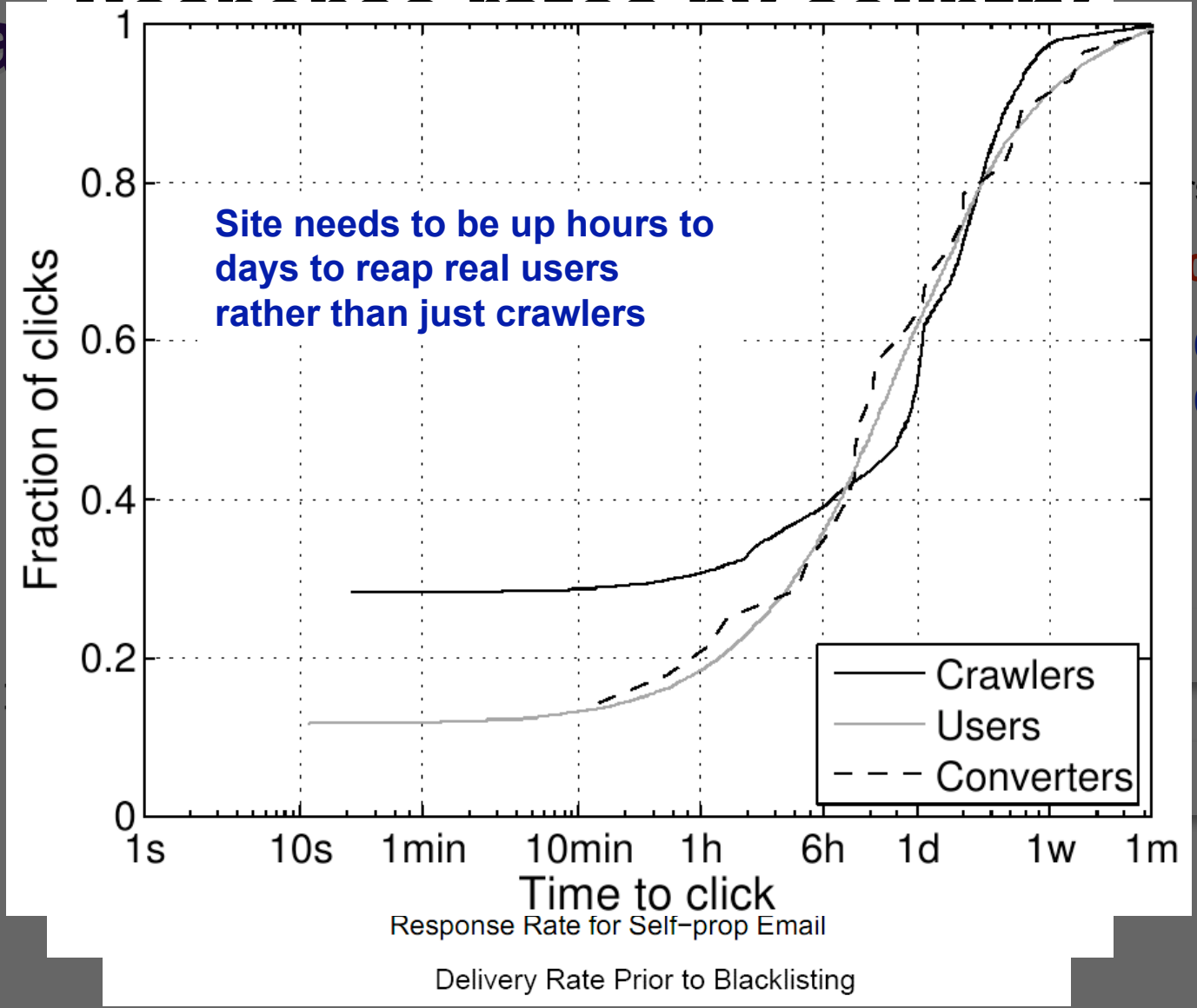
targeted

sions

0008%)

037%)

056%)



Response Rate for Self-prop Email

Delivery Rate Prior to Blacklisting

The Spammer's Bottom Line

- 28 purchases in 26 days, avg. "sale" ~$100
  - Total: $2,731.88, $140/day
- **But**: we interposed on only ~1.5% of workers:
  - $9,500/day (8,500 new bots per day)
  - $3.5M/year (back of envelope - be very careful!)
    - Though if selling Viagra via *Glavmed affiliation*, cut is **40%**
- Storm: service provider or integrated operation?
  - Retail price of spam ~$80 per million
    - Pharmacy spam would have cost 10x the profit!
  - Strongly suggests Storm operates as an integrated operation rather than a reseller