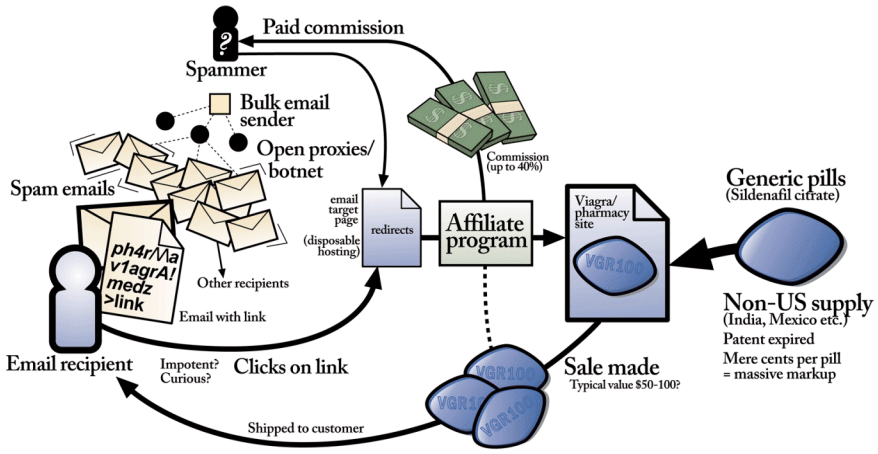
Anatomy of a modern Pharma spam campaign



Courtesy Stuart Brown
modernlifeisrubbish.co.uk

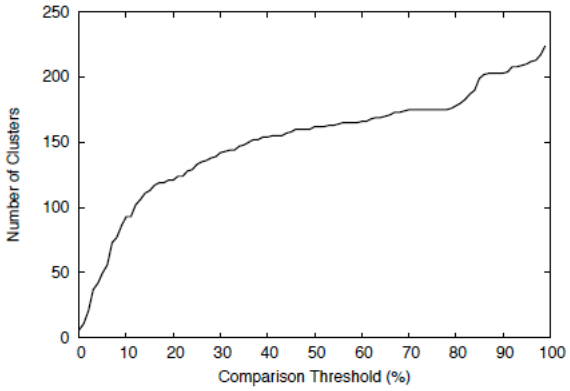


Figure 4: The choice of a threshold value for image shingling determines the number of clusters.

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.

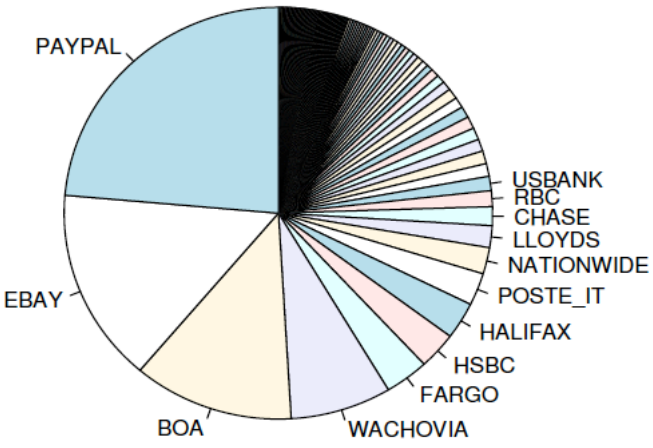


Figure 7: Proportion of ordinary phishing sites impersonating each bank.

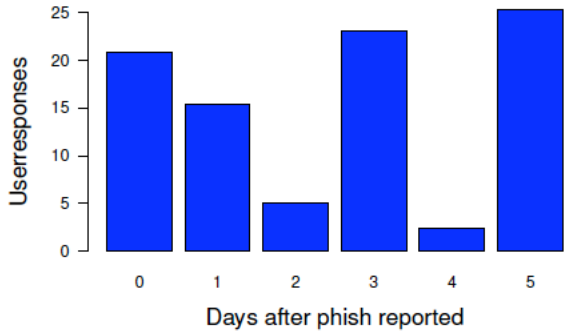
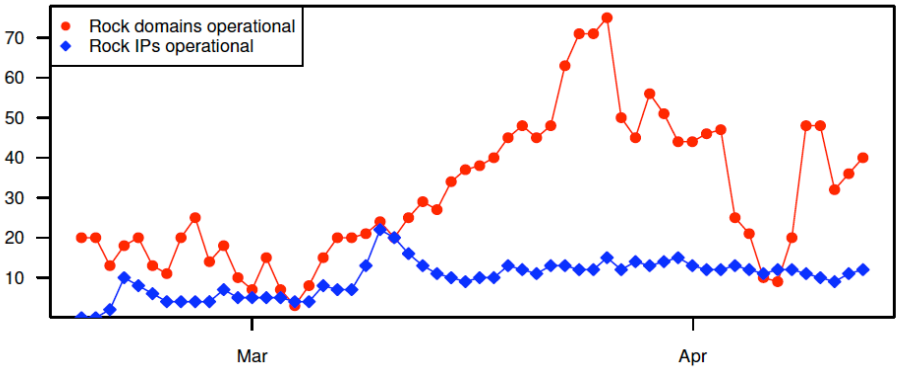
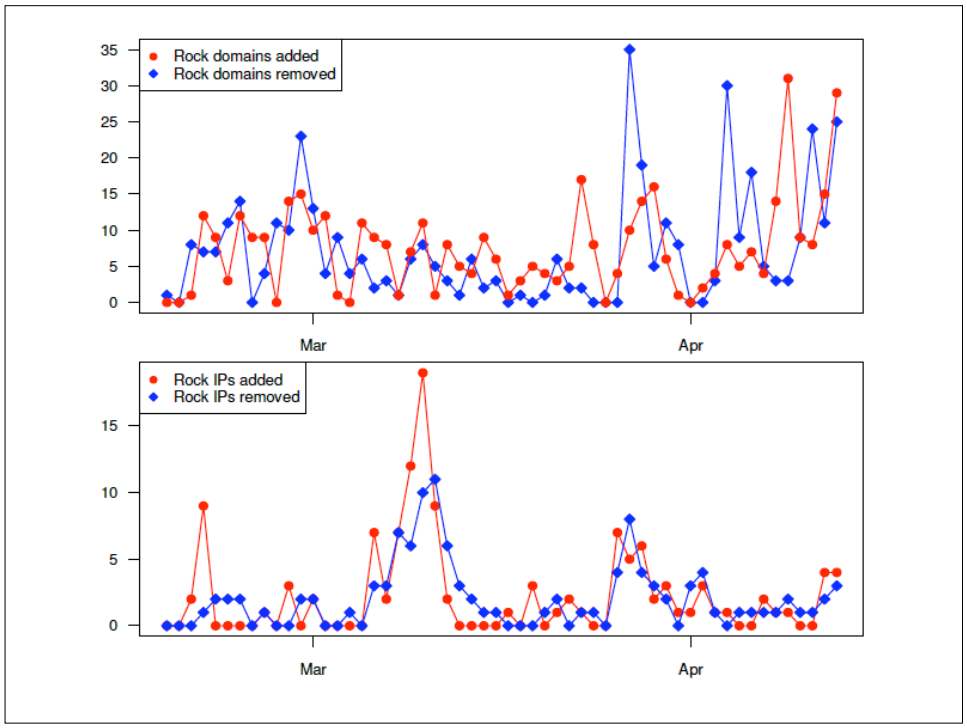
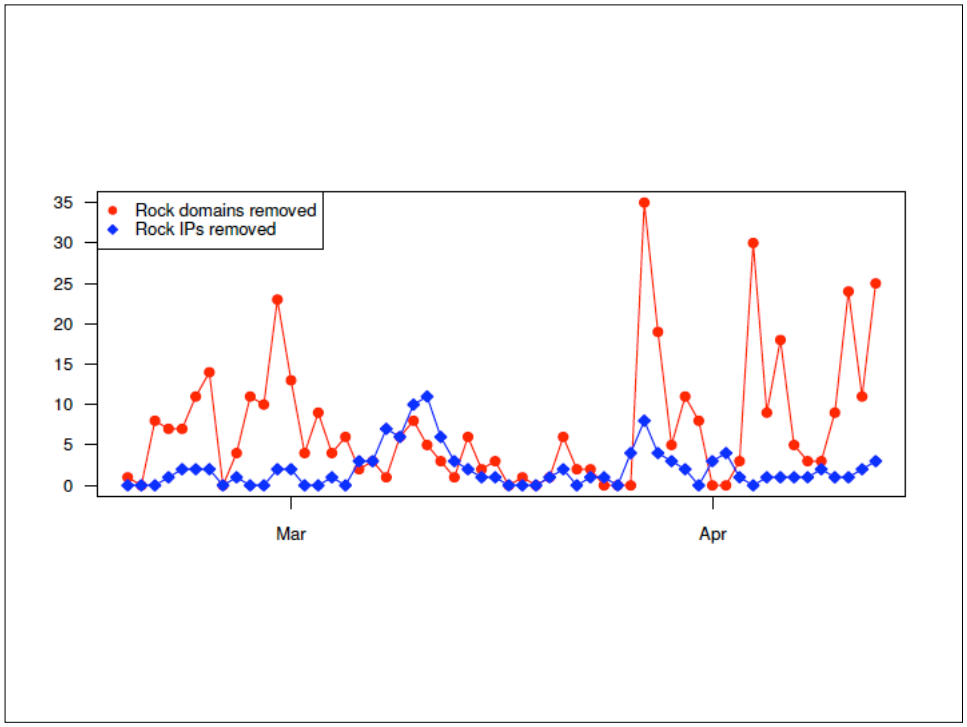


Figure 5: User responses to phishing sites over time. Data includes specious responses.




Rock domains added
Rock domains removed
35
30
25
20
15
10
5
0
Mar
Apr
Rock IPs added
Rock IPs removed
15
10
5
0
Mar
Apr


Rock domains removed
Rock IPs removed
35
30
25
20
15
10
5
0
Mar
Apr

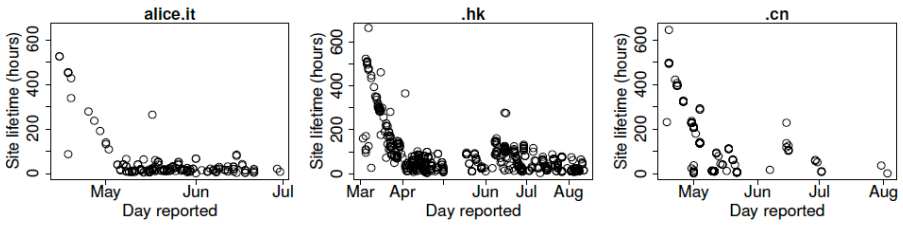


Figure 9: Scatter plot of phishing site lifetimes over time.

Table 2. Phishing Website Lifetimes by Attack Type

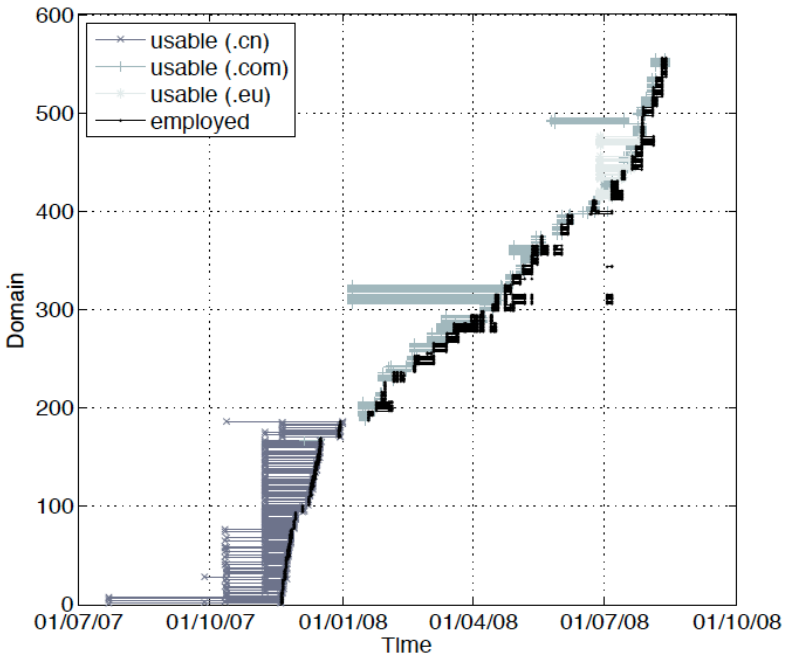
-	Sites	Lifetime (hours)	
		Mean	median
Free web-hosting			
all	395	47.6	0
brand owner aware	240	4.3	0
brand owner missed	155	114.7	29
Compromised machines			
all	193	49.2	0
brand owner aware	105	3.5	0
brand owner missed	155	103.8	10

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

Table 4. Website Lifetimes by Type of Offending Content

-	Period	Sites	Lifetime (hours)	
			mean	median
Child sexual abuse images	Jan–Dec 2007	2585	719	288
Phishing				
Free web-hosting (two brands)	Jan 2008	240	4.3	0
Compromised machines (two brands)	Jan 2008	105	3.5	0
Rock-phish domains (all brands)	Jan 2008	821	70.3	33
Fast-flux domains (all brands)	Jan 2008	314	96.1	25.5
Fraudulent websites				
Escrow agents	Oct–Dec 2007	696	222.2	24.5
Mule-recruitment websites	Mar 07–Feb 08	67	308.2	188
Fast-flux pharmacies	Oct–Dec 2007	82	1370.7	1404.5



Are Bots & Spam the New Black Gold?

Storm worm 'making millions a day'

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

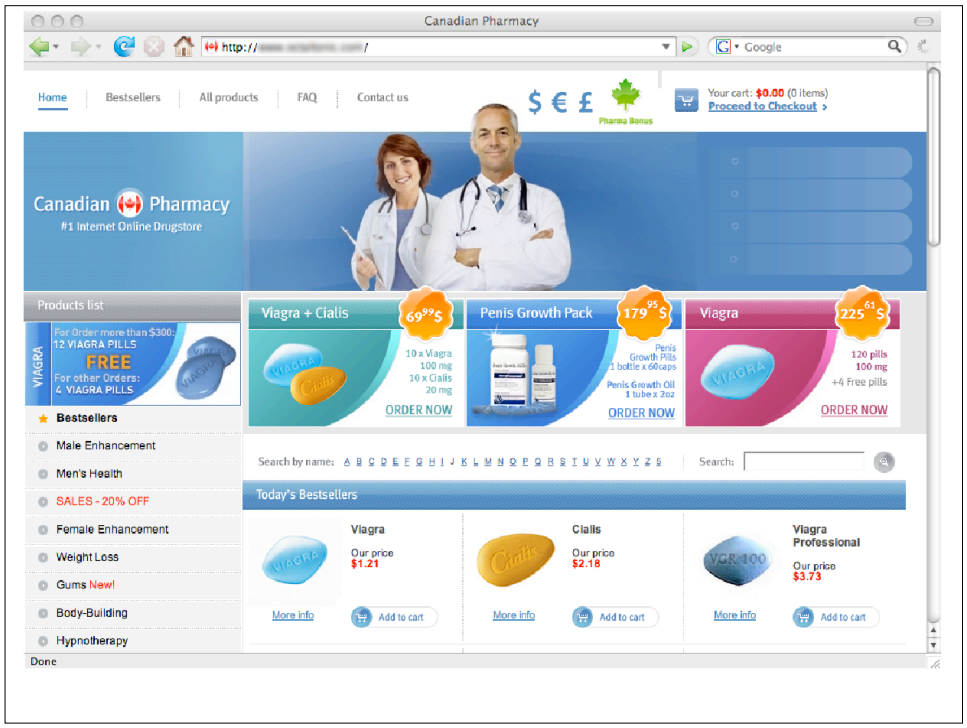
Clive Akass, Personal Computer World 11 Feb 2008

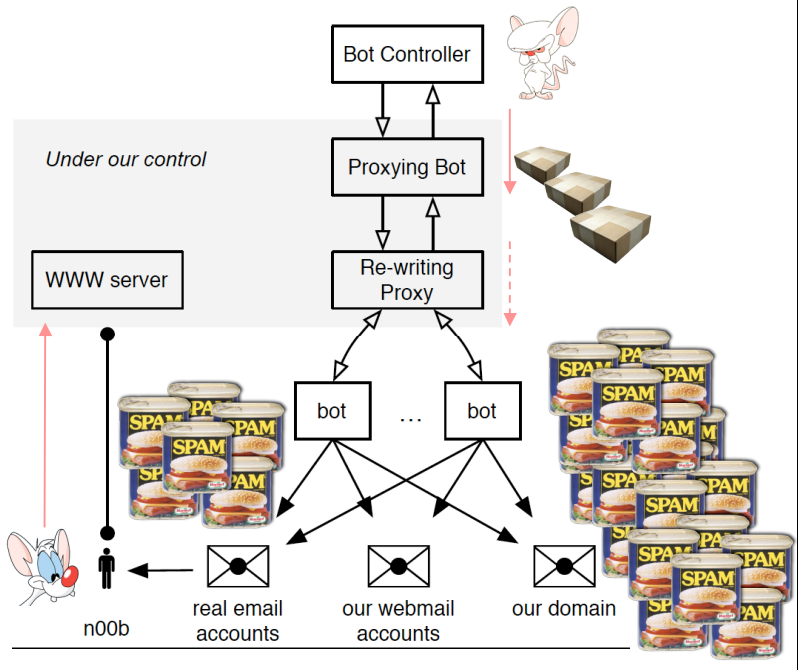
The people behind the Storm worm are making millions of pounds a day by using it to generate revenue, according to IBM's principal web security strategist.

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

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

How can we **measure** this?


Canadian Pharmacy
Home
Bestsellers
All products
FAQ
Contact us
Your cart: $0.00 (0 items)
Proceed to Checkout
Canadian Pharmacy
#1 Internet Online Drugstore
Products list
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:
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

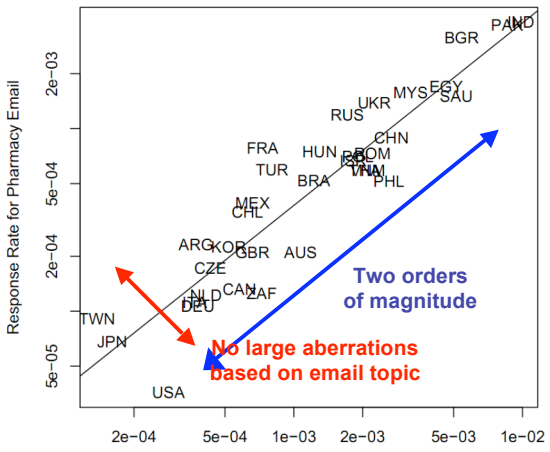

Bot Controller
Under our control
Proxying Bot
WWW server
Re-writing Proxy
bot
…
bot
SPAM
n00b
real email accounts
our webmail accounts
our domain

Spam conversion experiment

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

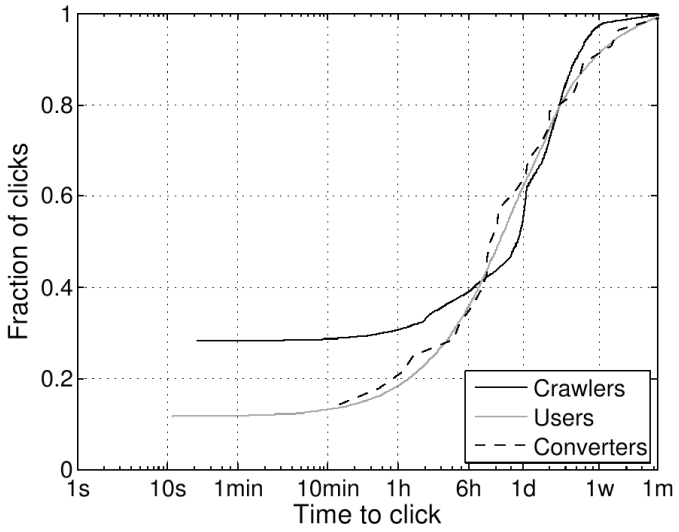
	Pharmacy Campaign	E-card Campaigns	
		Postcard	April Fool
Worker bots	31,348	17,639	3,678
Emails	347,590,389	83,665,479	38,651,124
Duration	19 days	7 days	3 days

Response rates by country



Delivery Rate Prior to Blacklisting

Time-to-click distribution



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