Spam & Spammer Profits

CS 161 - Computer Security

Profs. Vern Paxson & David Wagner

TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

http://inst.eecs.berkeley.edu/~cs161/

April 21, 2010

Thinking About Economics

- Given the rise of cybercrime-fueled Internet attacks, where should we be investing our limited security resources?
  - Preventing host compromise?
  - Policing networks, rolling up botnets?
  - Other?
- We have structural disadvantages
  - Defenses public, attacker develops/tests in private
    - Arms race where best case for defender is to “catch up”
  - Attacker not tied to any particular technology; cheaper for them to change than us
  - Minimal deterrence
  - **Significant value proposition for attacker**

Thinking About Economics, con't

- Given the rise of cybercrime-fueled Internet attacks, where should we be investing our limited security resources?

Premise:
We're unlikely to spend efficiently until we understand the economics of the bad guy

- We have structural disadvantages
  - Defenses public, attacker develops/tests in private
    - Arms race where best case for defender is to "catch up"
  - Attacker not tied to any particular technology; cheaper for them to change than us
  - Minimal deterrence
  - **Significant value proposition for attacker**

Monetizing Spam

- In what ways can spammers make money off of sending spam?
  - And who has incentives to thwart these?
    - (Other than law enforcement)
- Scheme #1: advertise goods or services
  - Examples: fake Rolexes, Viagra, university degrees
  - Profit angle: increased sales
  - Who'll try to stop: brand holders
- Scheme #2: phishing
  - Profit angle: transfer $$$ out of accounts; sell accounts to others; use accounts for better spamming (e.g. Facebook)
  - Opponents: issuers of accounts
  - Note: targeted phishing ("spear-phishing") doesn't actually need much in the way of spam due to low volume

Monetizing Spam, con't

- Scheme #3: scams
  - Examples: pen pal relationships, 419 ("Nigerian")
  - Profit angle: con victim into sending money
  - Opponents: scambaiters (419eater.com)
- Scheme #4: recruiting crooks/underlings
  - Examples: money mules, reshippers
  - Profit angle: more efficient cybercrime
  - Opponents: ?
- Scheme #5: recruiting bots
  - Examples: "important security patch!", "someone sent you a greeting card!"
  - Profit angle: get malware installed on new machines
  - Opponents: ?

Monetizing Spam, con't

- Scheme #6: pump-and-dump
  - Example: "Falcon Energy (FPK) is about to go through the roof! Don't miss out on $eriou$ Profit$!"
  - Profit angle: penny-stock momentarily goes up, dump pre-bought shares when it does
  - Opponents: Securities and Exchange Commission
  - Note: unlike other monetization techniques, the "back channel" is out-of-band
    - No link in messages back to the scammer

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*

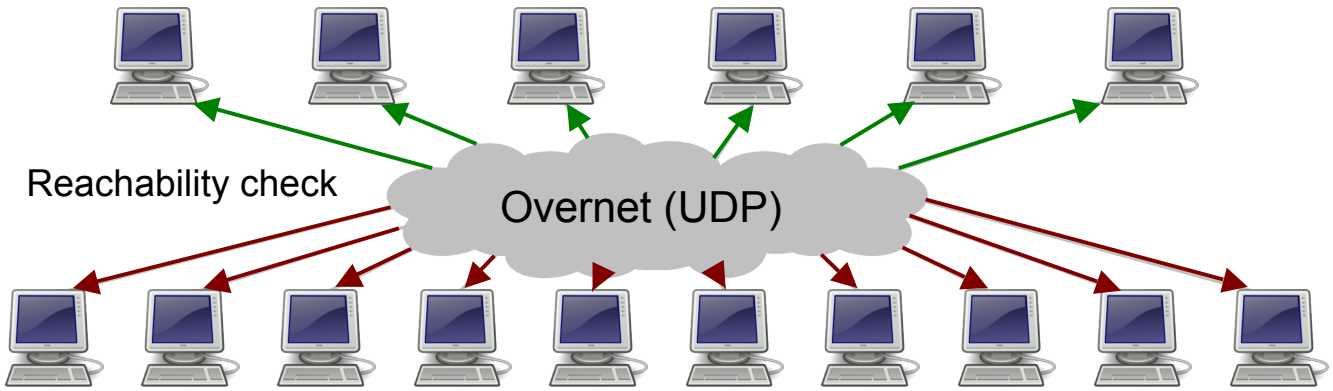
Welcome to **Storm**!

Would you like to be one of our newest bots?

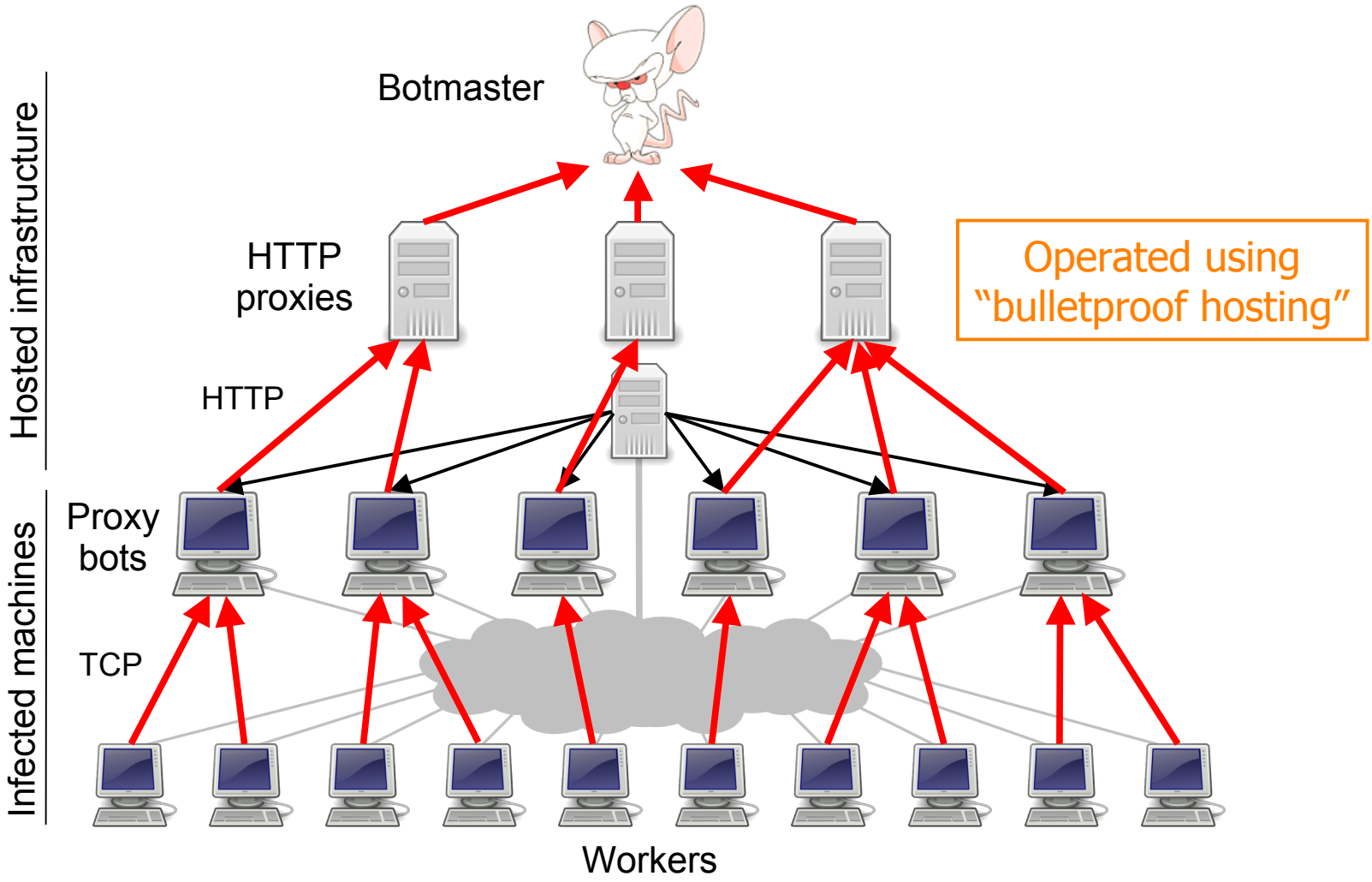
Just read your postcard!

(Or even easier: just wait 5 seconds!)

The Storm botnet



The Storm botnet



Google translate | http://goohost.ru/ | Translate | Help | Sign in

Translate from: Russian | Translate into: English | View: Translation Original

GooHost.ru

Reliable and quality hosting

Тел.: +7(495) 542-39-87, icq: 418396204

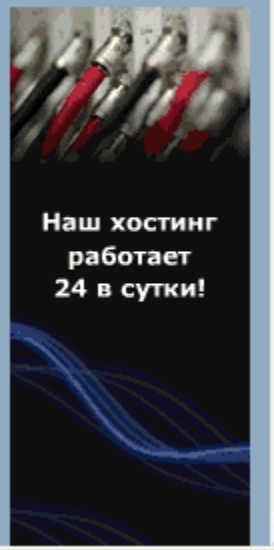
Menu

- Hosting Plans
- Email Mailing
- Website Design
- FAQ
- Dedicated server
- Domain Registration
- Payment
- Contact

Hosting Plans

We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.

We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.



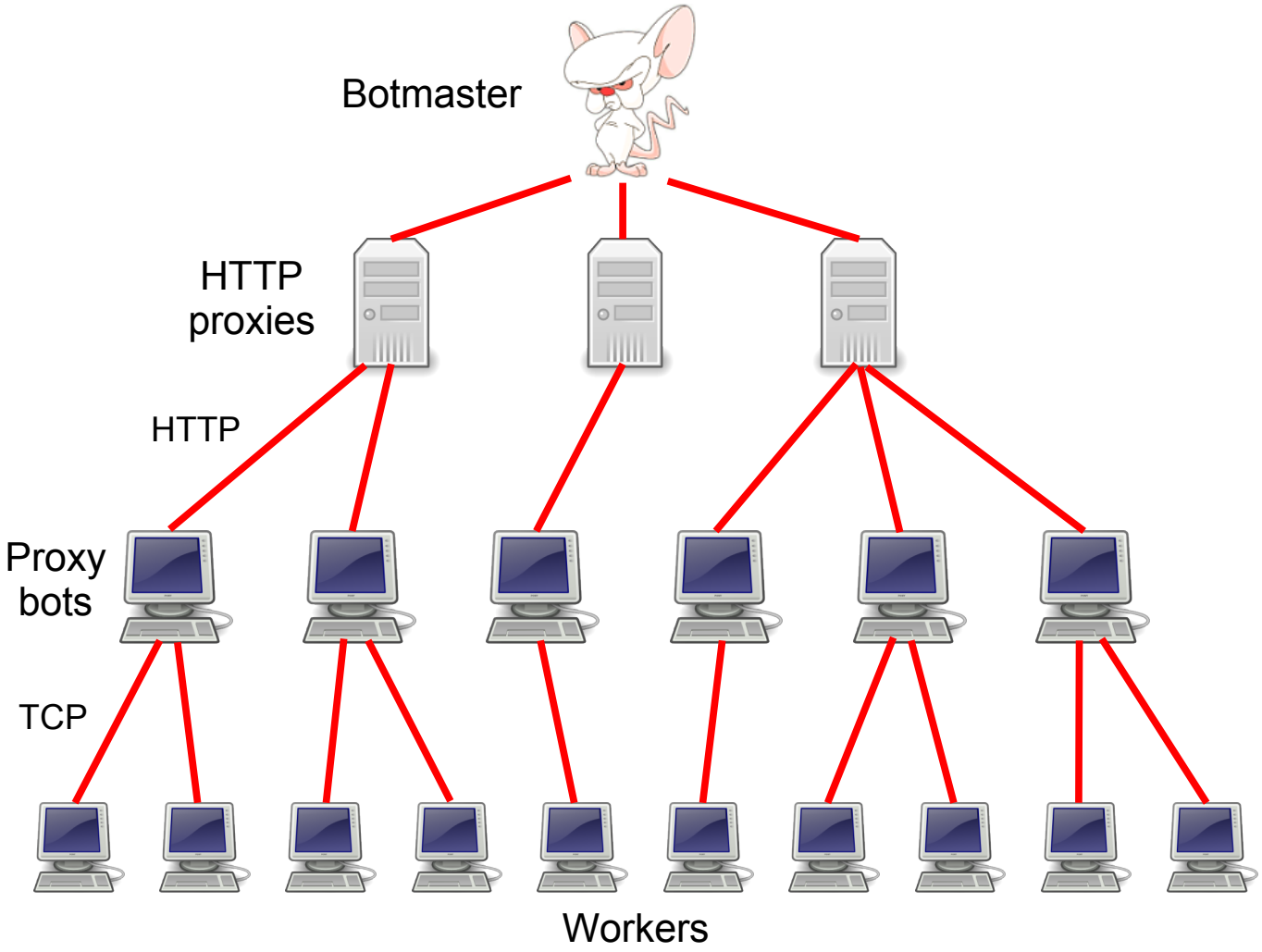
Internet

Obuzoustoychivy hosting is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

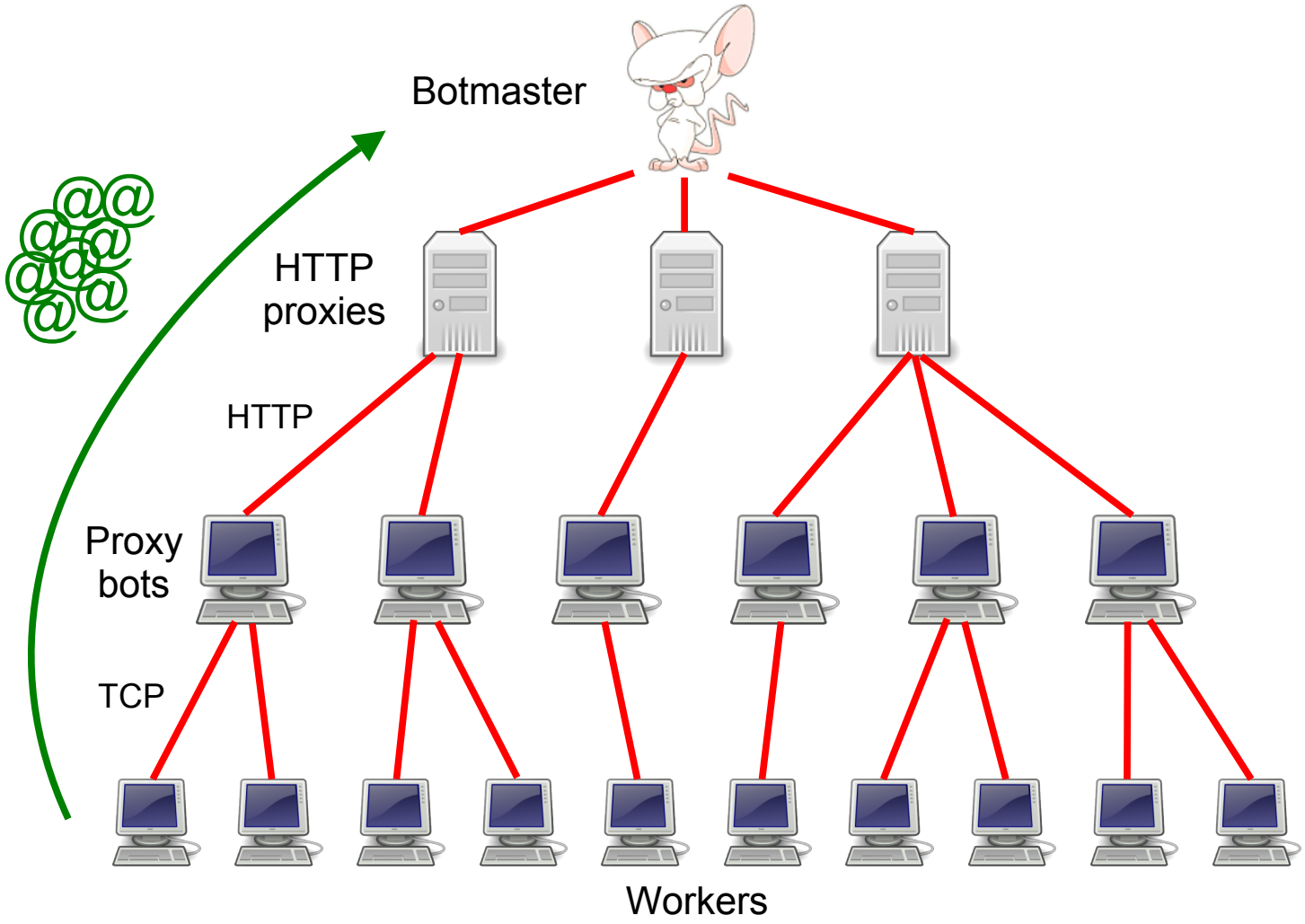
MINI PLAN	
Volume disc	400 MB
Domains	1
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	4 000 rub. / 1 month.

STARTER PLAN	
Volume disc	500 mb
Domains	3
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	5 000 rub. / 1 month.
BUSINESS PLAN	
Volume disc	1000 mb
Domains	7
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	7 000 rub. / 1 month.
PREMIUM PLAN	

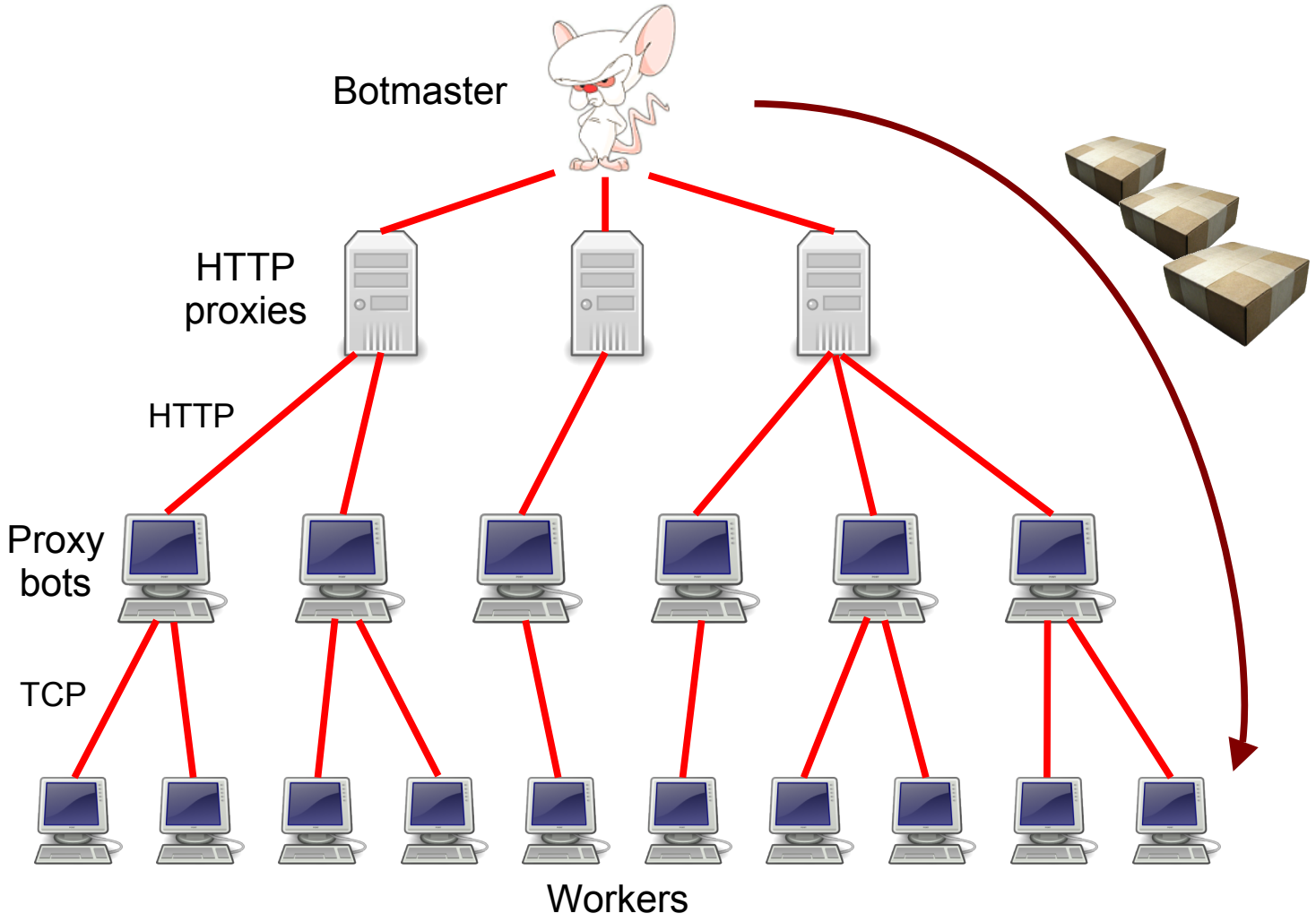
Spam campaign mechanics



Campaign mechanics: harvest



Campaign mechanics: spamming



MACRO	SEEN LIVE	FUNCTIONALITY
(0)	✓	Spam target email address.
(A)	✓	FQDN of sending bot, as reported to the bot as part of the preceding C&C exchange.
(B)		Creates content-boundary strings for multi-part messages.
(C*num*)	✓	Labels a field's resulting content, so it can be used elsewhere through (V); see below.
(D)	✓	Date and time, formatted per RFC 2822.
(E)		ROT-3–encodes the target email address.
(F*string*)	✓	Random value from the dictionary named *string*.[2]
(G*string*)	✓	Line-wrap *string* into 72 characters per line.
(H*string*)		Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts.
(I)	✓	Random number between 1 and 255, used to generate fake IP addresses.
(J*string*)		Produces quoted-printable "=20" linewrapping.
(K)		IP address of SMTP client.
(M)	✓	6-character string compatible with Exim's message identifiers (keyed on time).
(N)		16-bit prefix of SMTP client's IP address.
(O*string*:*num*)	✓	Randomized message identifier element compatible with Microsoft SMTPSVC.
(Pnum_1[-num_2]:*string*)	✓	Random string of num_1 (up to num_2, if provided) characters taken from *string*.
(Q*string*)		Quoted-printable "=" linewrapping.
(Rnum_1-num_2)	✓	Random number between num_1 and num_2. Note, special-cased when used with (D).
(U*string*)		Randomized percent-encoding of *string*.
(V*num*)	✓	Inserts the value of the field identified by (C*num*).
(W)		Time and date as plain numbers, e.g. "20080225190434".
(X)		Previously selected member of the "names" dictionary.
(Y*num*)	✓	8-character alphanumeric string, compatible with Sendmail message identifiers.
(Z)	✓	Another Sendmail-compatible generator for message identifiers.

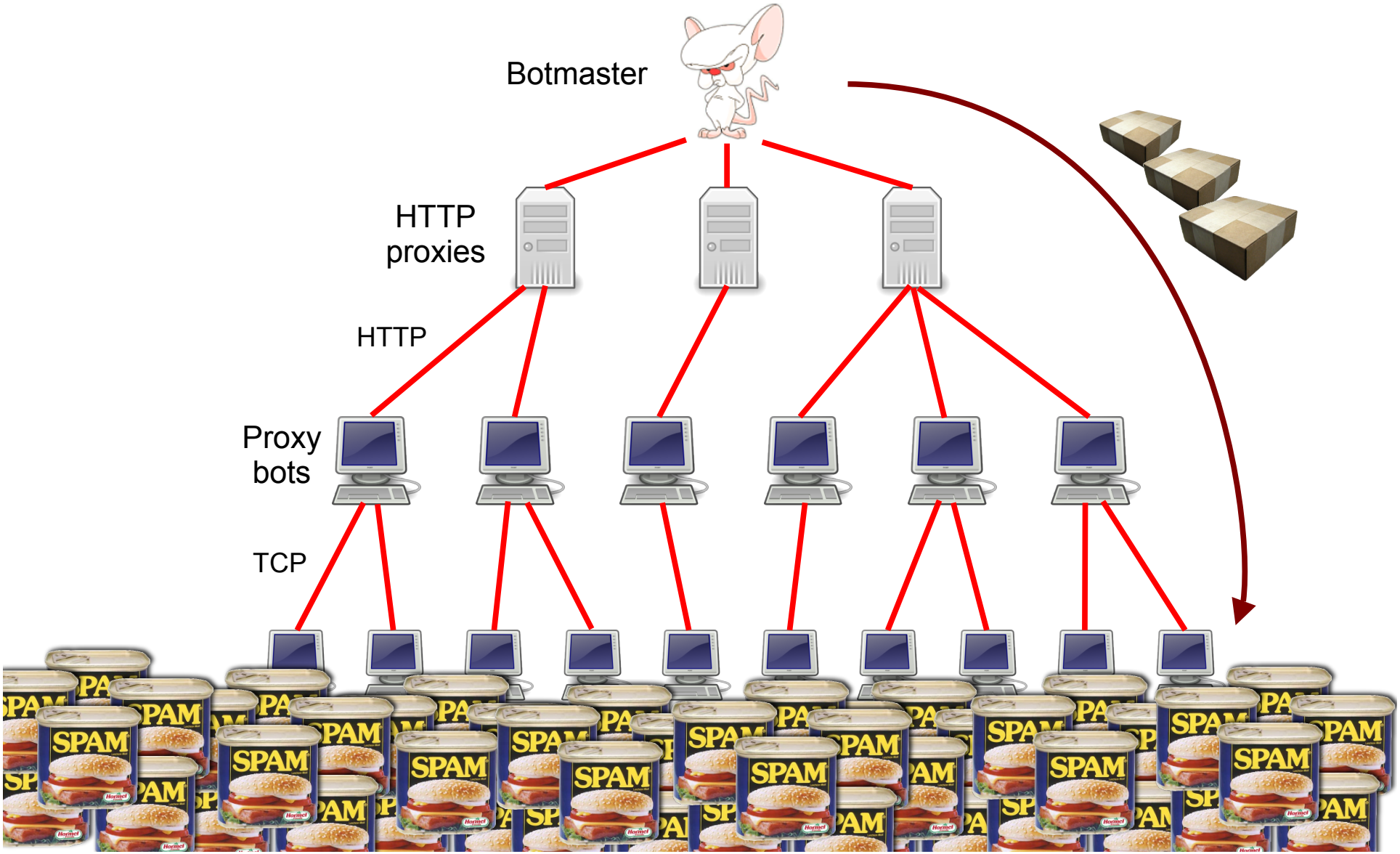
Table 2: Storm's spam-generation templating language.

```
Received: from %^C0%^P%^R2-6^%:qwertyuiopasdfghjklzxcvbnm^%.%^P%^R2-6^%:qwertyuiopasdfghjkl ▷
                                                zxcvbnm^%^% ([%^C6%^I^%.%^I^%.%^I^%.%^I^%^%]) by ▷
                                                %^A^% with Microsoft SMTPSVC(%^Fsvcver^%); %^D^%
Message-ID: <%^O%^V6^%:%^R3-50^%^%%^V0^%>
From: <%^Fnames^%@%^Fdomains^%>
To: <%^0^%>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: %^D-%^R30-600^%^%
```

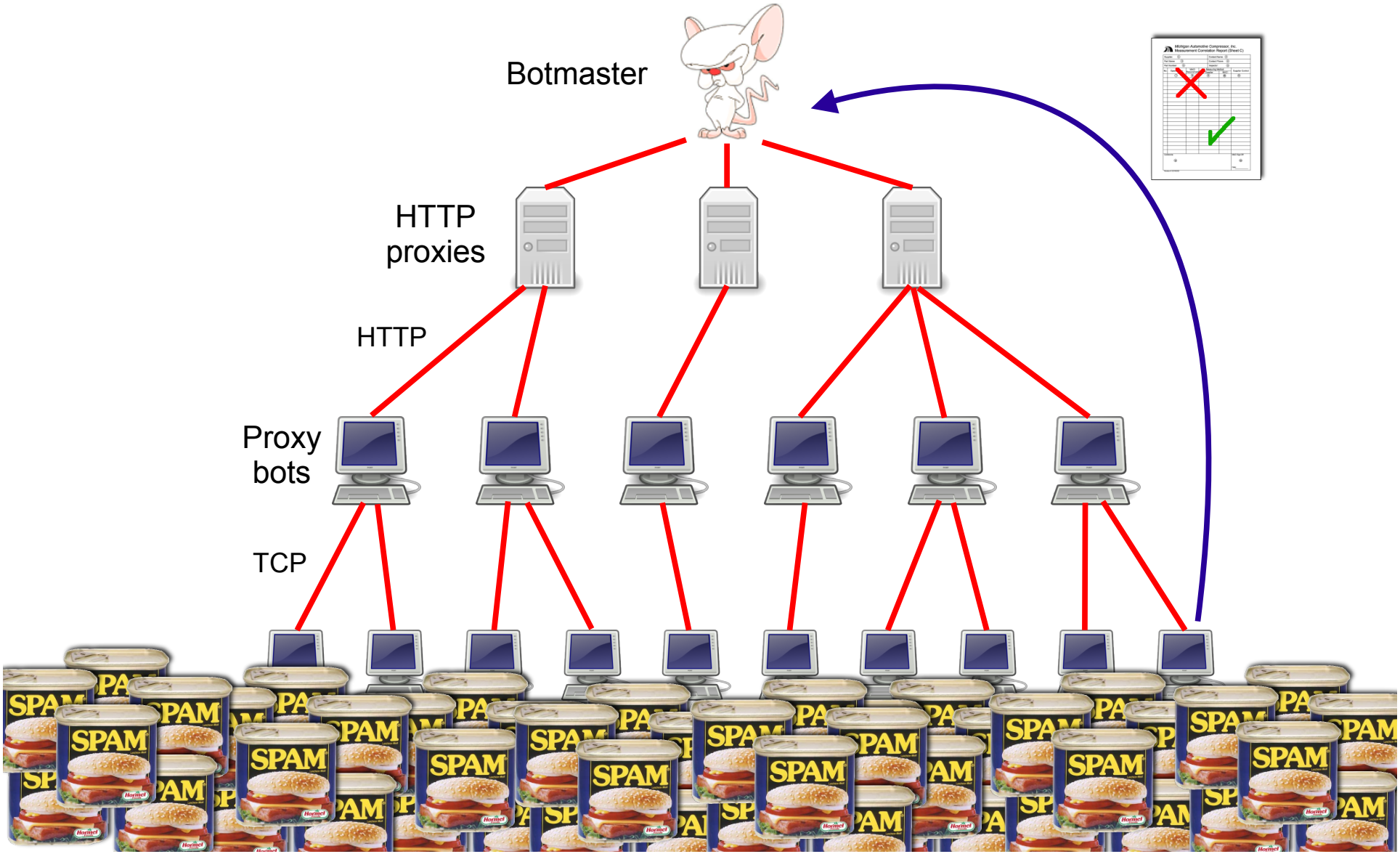
```
Received: from auz.xwzww ([132.233.197.74]) by dsl-189-188-79-63.prod-infinitum.com.mx with ▷
                          Microsoft SMTPSVC(5.0.2195.6713); Wed, 6 Feb 2008 16:33:44 -0800
Message-ID: <002e01c86921$18919350$4ac5e984@auz.xwzww>
From: <katiera@experimentalist.org>
To: <voelker@cs.ucsd.edu>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: Wed, 6 Feb 2008 16:33:44 -0800
```

Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The ▷-symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.

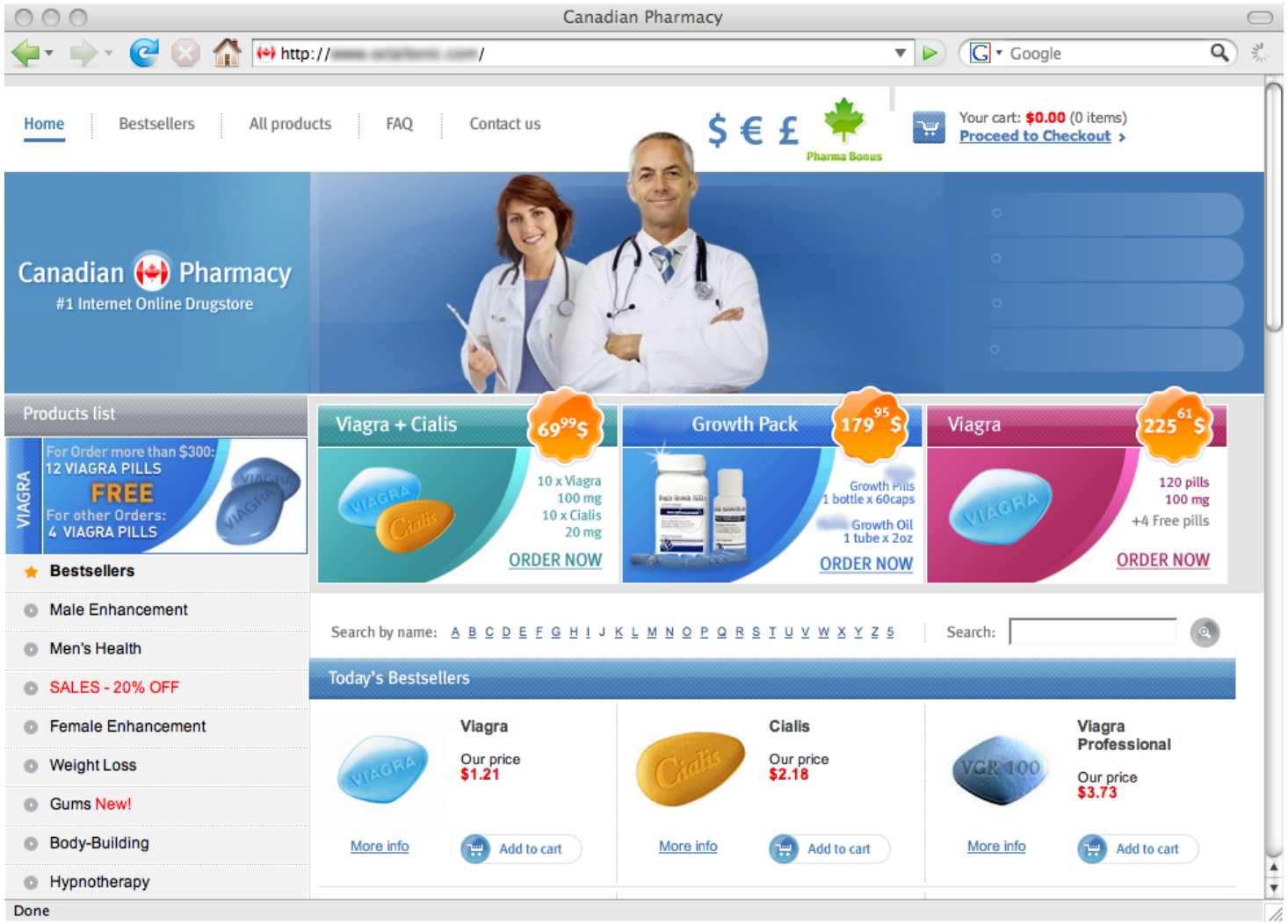
Campaign mechanics: spamming



Campaign mechanics: reporting



Welcome to **Storm**! What can we sell you?



Anatomy of a modern Pharma spam campai

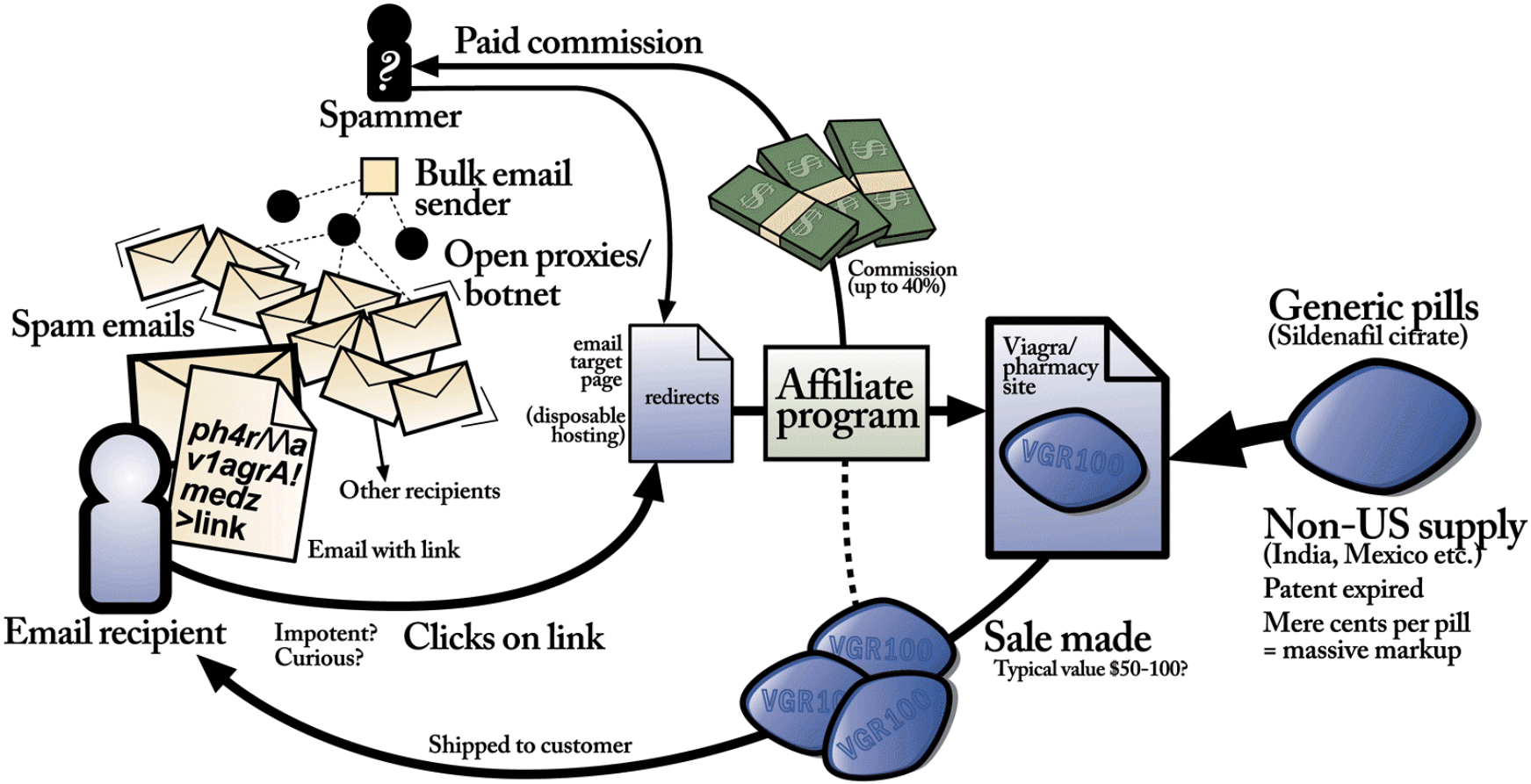
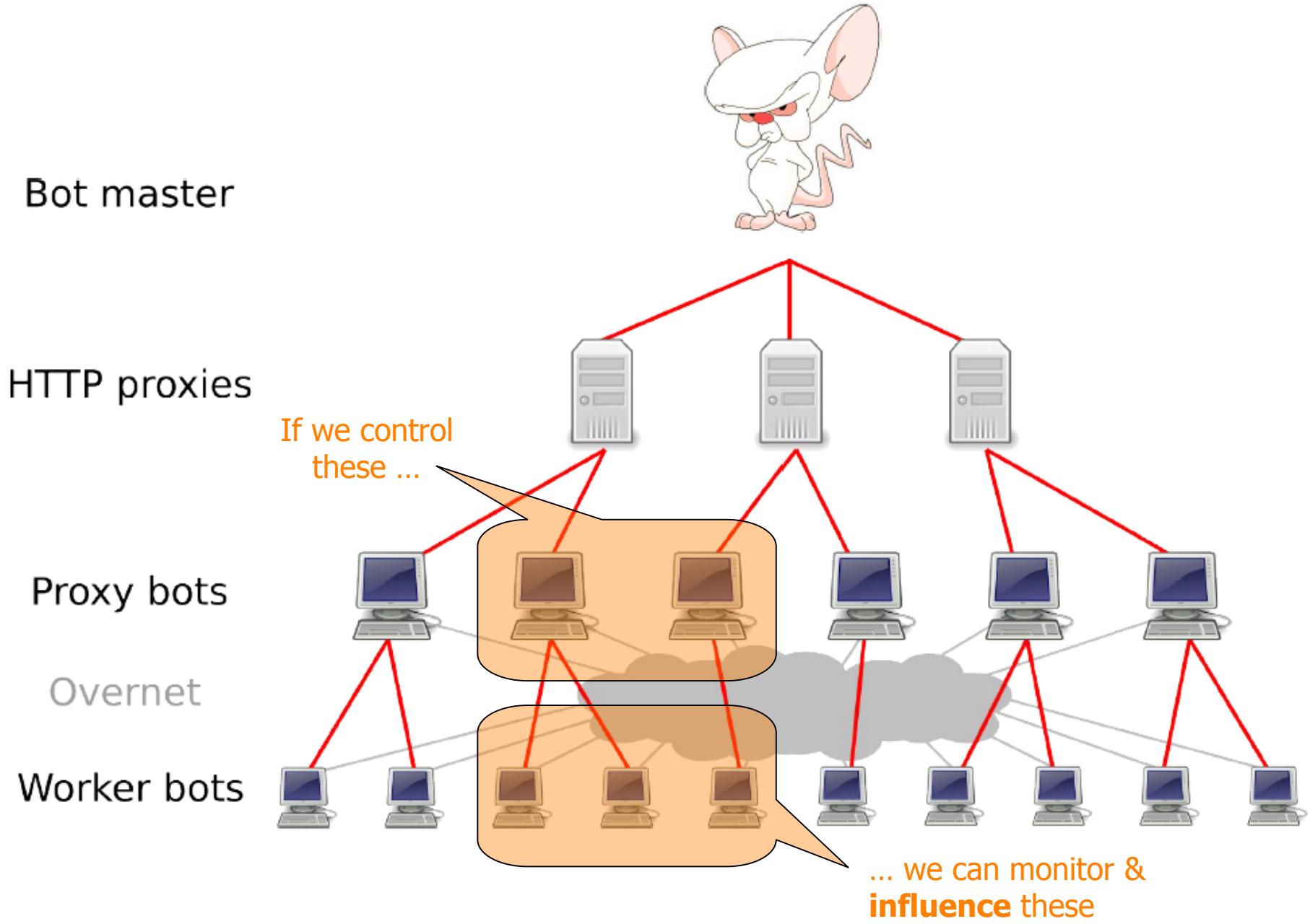


Diagram by Stuart Brown
modernlifeisrubbish.co.uk

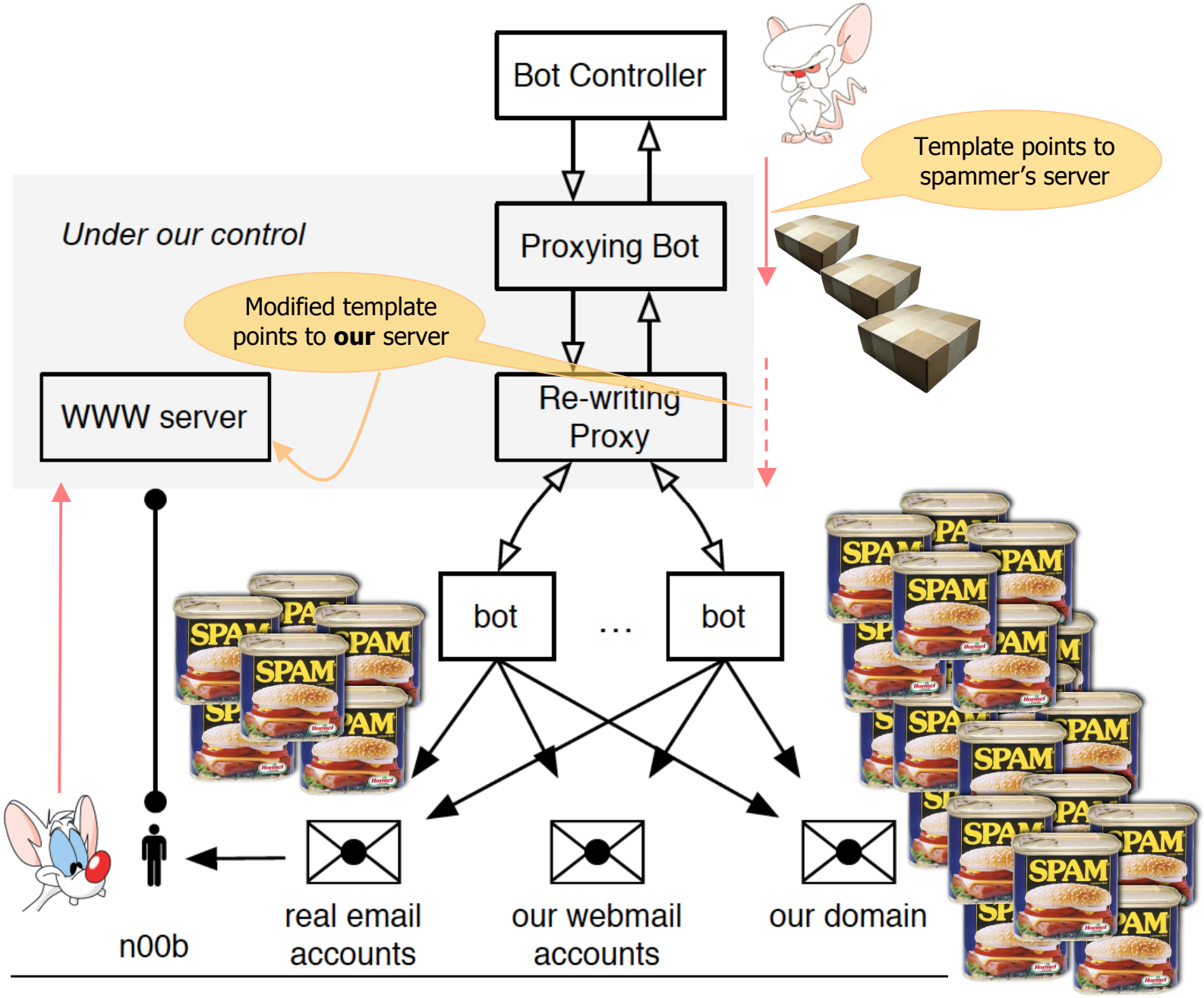
These folks seem trustworthy …

… how about these?


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

Botnet *infiltration*

- **Key idea:** distributed C&C is a ***vulnerability***
  - Botnet authors like de-centralized communications for scalability and resilience, but…
  - … to do so, they trust their bots to be good actors
  - If you can *modify* the right bots you can observe and influence actions of the botnet
- Thanks to *E-Card* spam, we can easily acquire Storm bot binaries …
  - … and run them within controlled **GQ** honeyfarm environment
- With a lot of elbow grease, we reverse-engineered the C&C protocol …
- … so we can record all C&C sent through us …

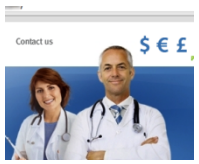

Bot Controller
Under our control
Proxying Bot
Template points to spammer's server
Modified template points to **our** server
WWW server
Re-writing Proxy
bot
…
bot
n00b
real email accounts
our webmail accounts
our domain

Spam conversion experiment

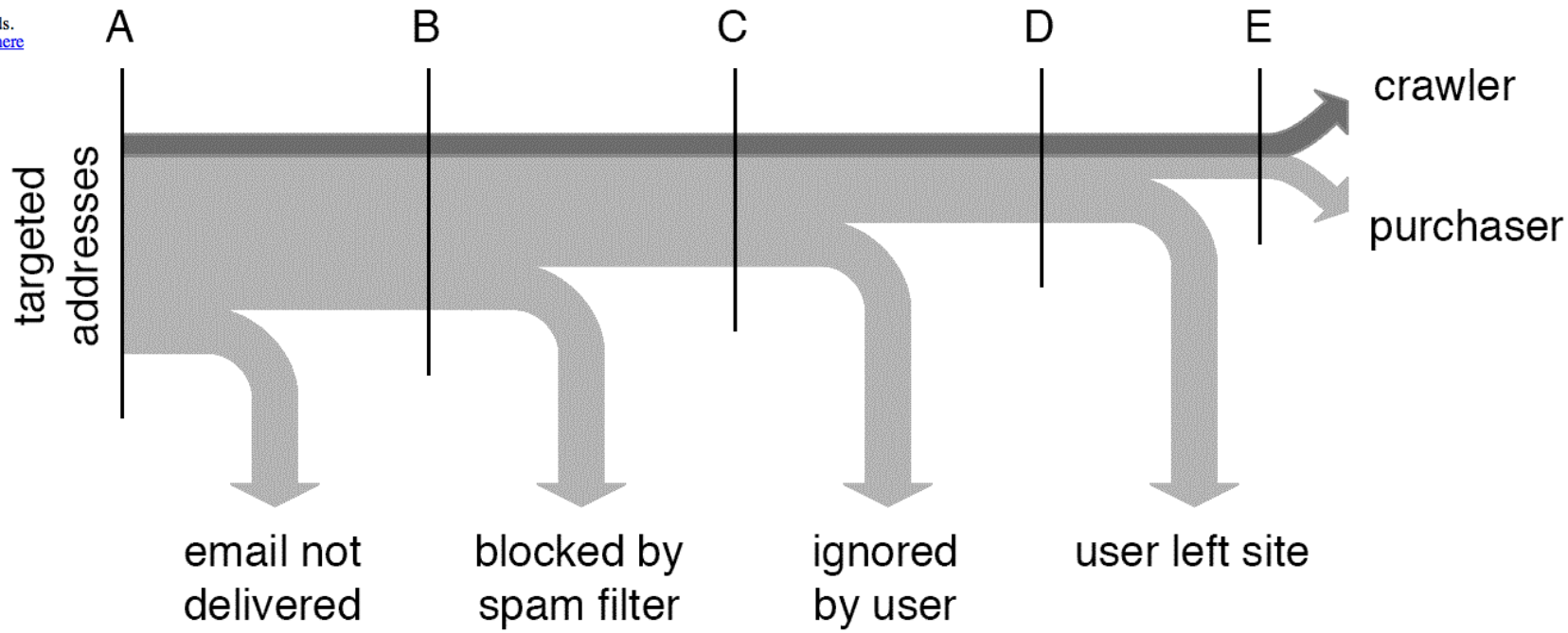
- Experimented with Storm March 21 – April 15, 2008
- Instrumented roughly 1.5% of Storm's total output

	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

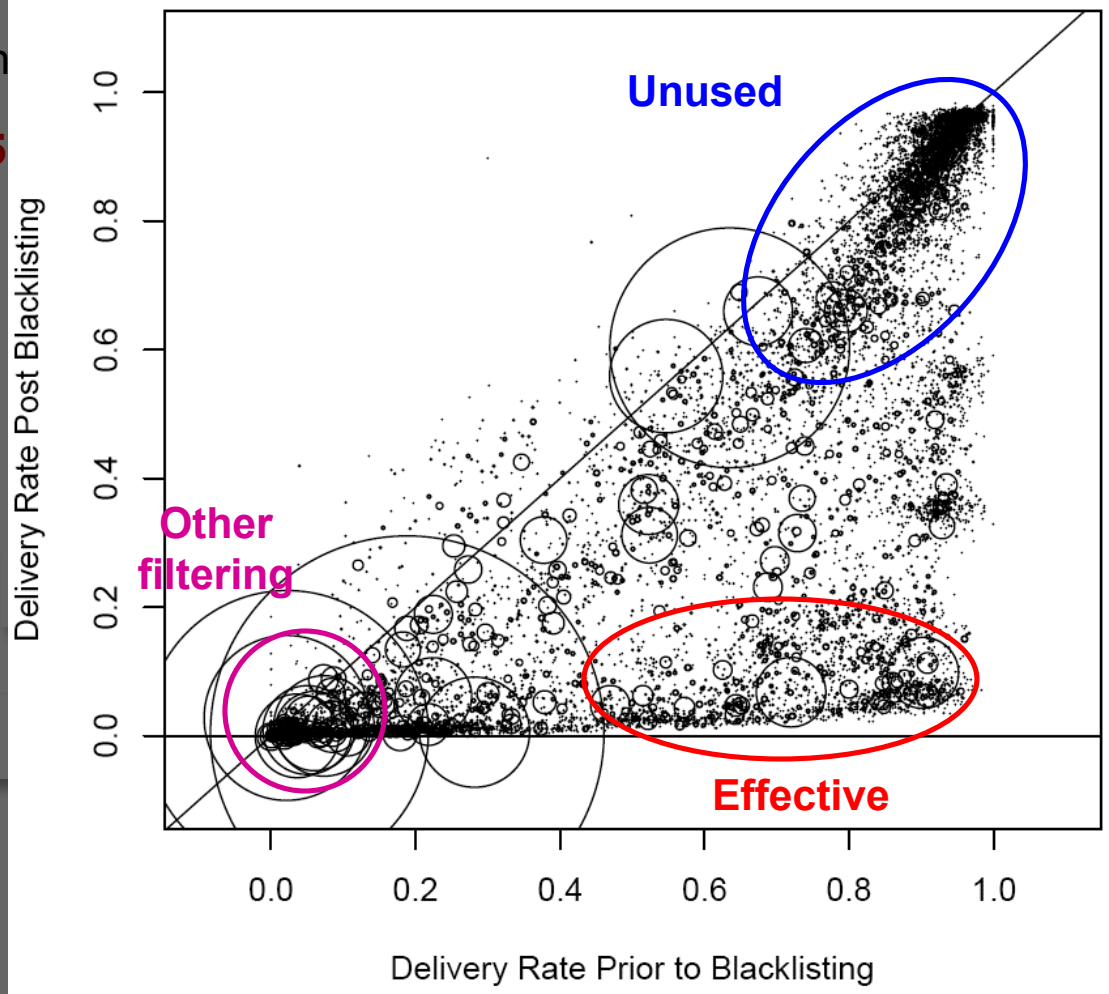
Spam pipeline



Sent	MTA	Inbox	Visits	Conversions
347.5M	82.7M (24%)		10,522 (0.003%)	28 (0.000008%)
83.6 M	21.1M (25%)		3,827 (0.005%)	316 (0.00037%)
40.1 M	10.1M (25%)	---	2,721 (0.005%)	225 (0.00056%)



Effects of Blacklisting (CBL Feed)



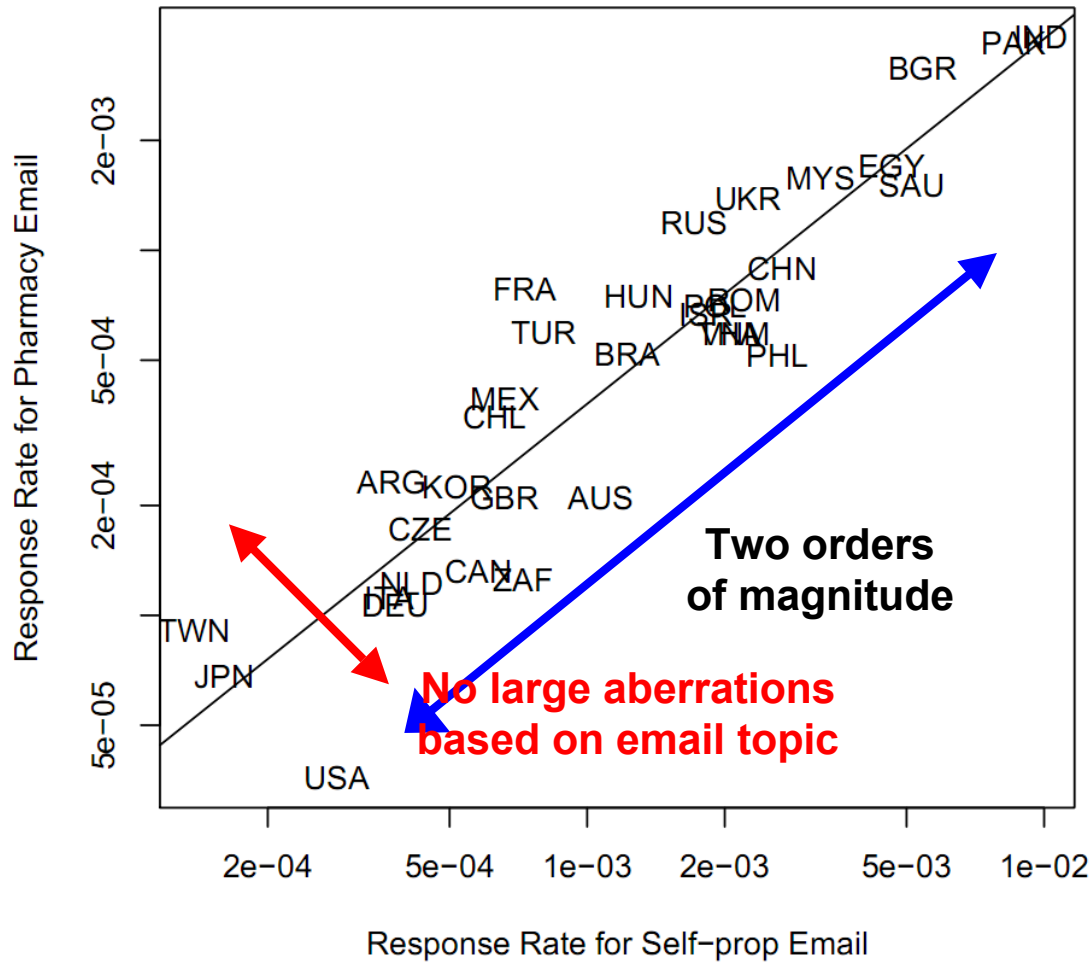
Spam filtering software

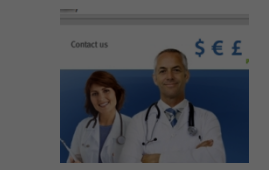
- The fraction of spam delivered into user inboxes depends on the spam filtering software used
  - Combination of site filtering (e.g., blacklists) and content filtering (e.g., spamassassin)
- Difficult to generalize, but we can use our test accounts for specific services

SPAM FILTER	PHARMACY	POSTCARD	APRIL FOOL
Gmail	0.00683%	0.00176%	0.00226%
Yahoo	0.00173%	0.000542%	none
Hotmail	none	none	none
Barracuda	0.131%	N/A	0.00826%

Fraction of spam sent that was delivered to inboxes

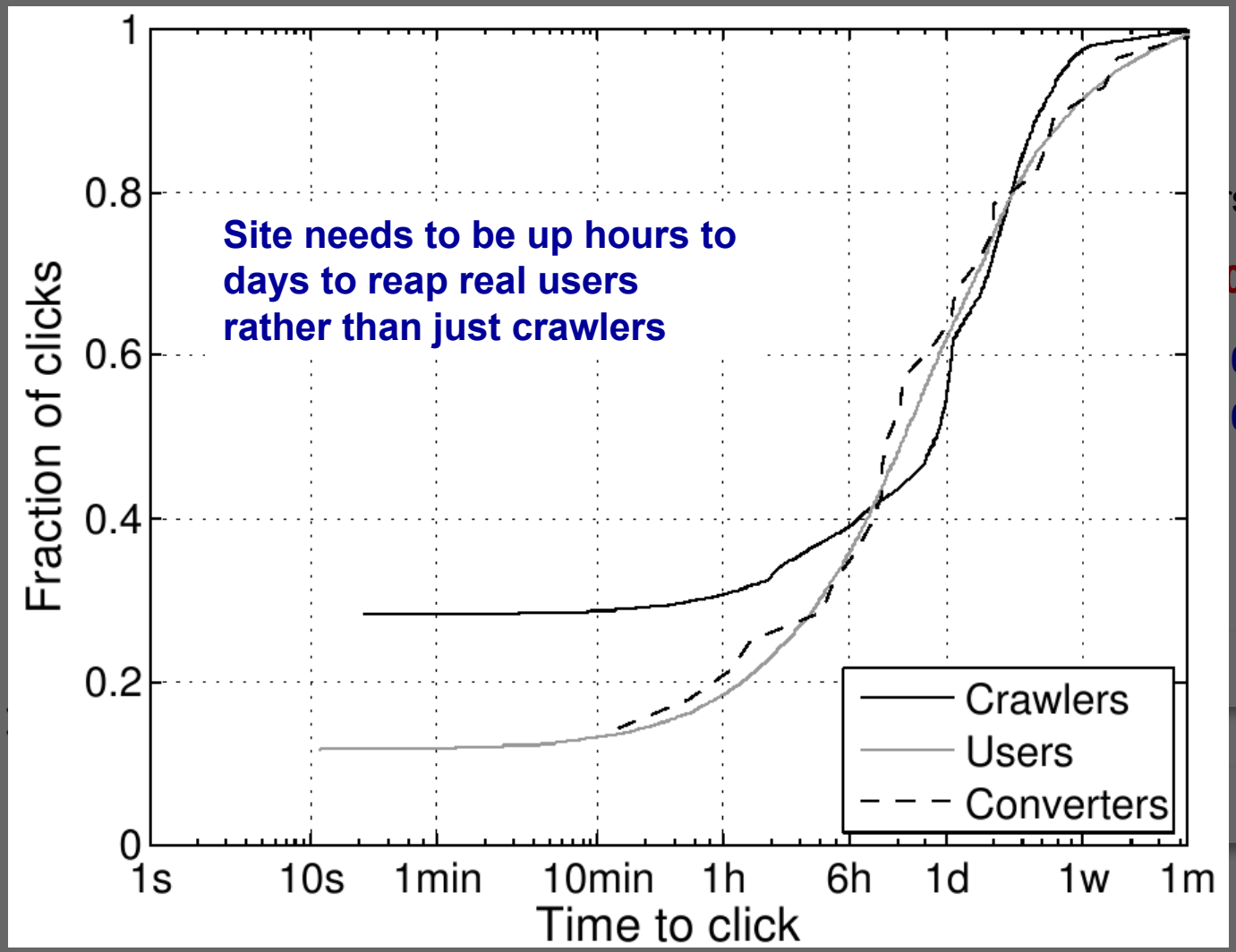
Response rates by country





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

targeted



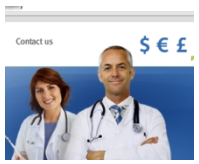
rsions

0008%)

037%)

056%)

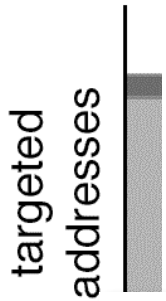
Spam pipeline



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

Sent	MTA	Inbox	Visits	Conversions
347.5M	82.7M (24%)		10,522 (0.003%)	28 (0.000008%)
83.6 M	21.1M (25%)		3,827 (0.005%)	316 (0.00037%)
40.1 M	10.1M (25%)	---	2,721 (0.005%)	225 (0.00056%)

A



Pharma: 12 M spam emails for one "purchase"

E-card: 1 in 10 visitors execute the binary

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