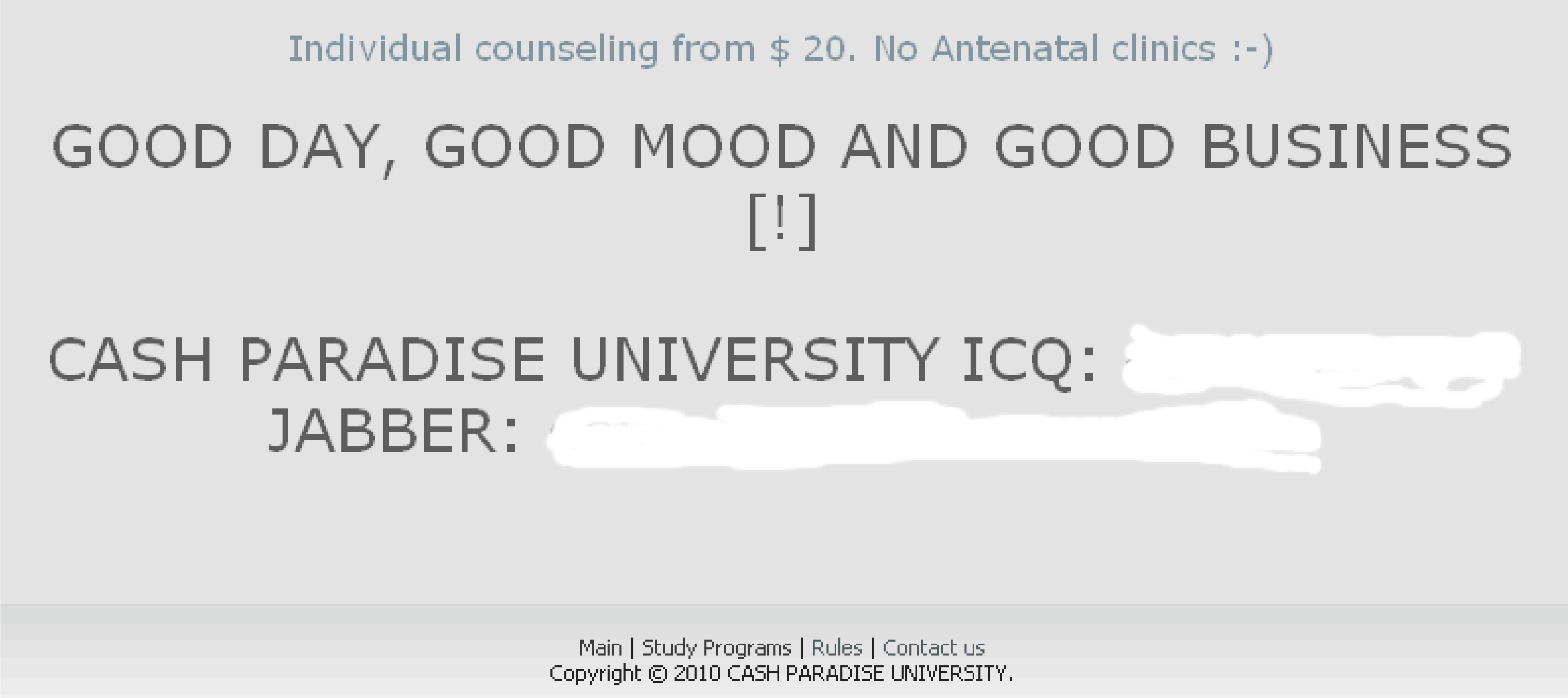
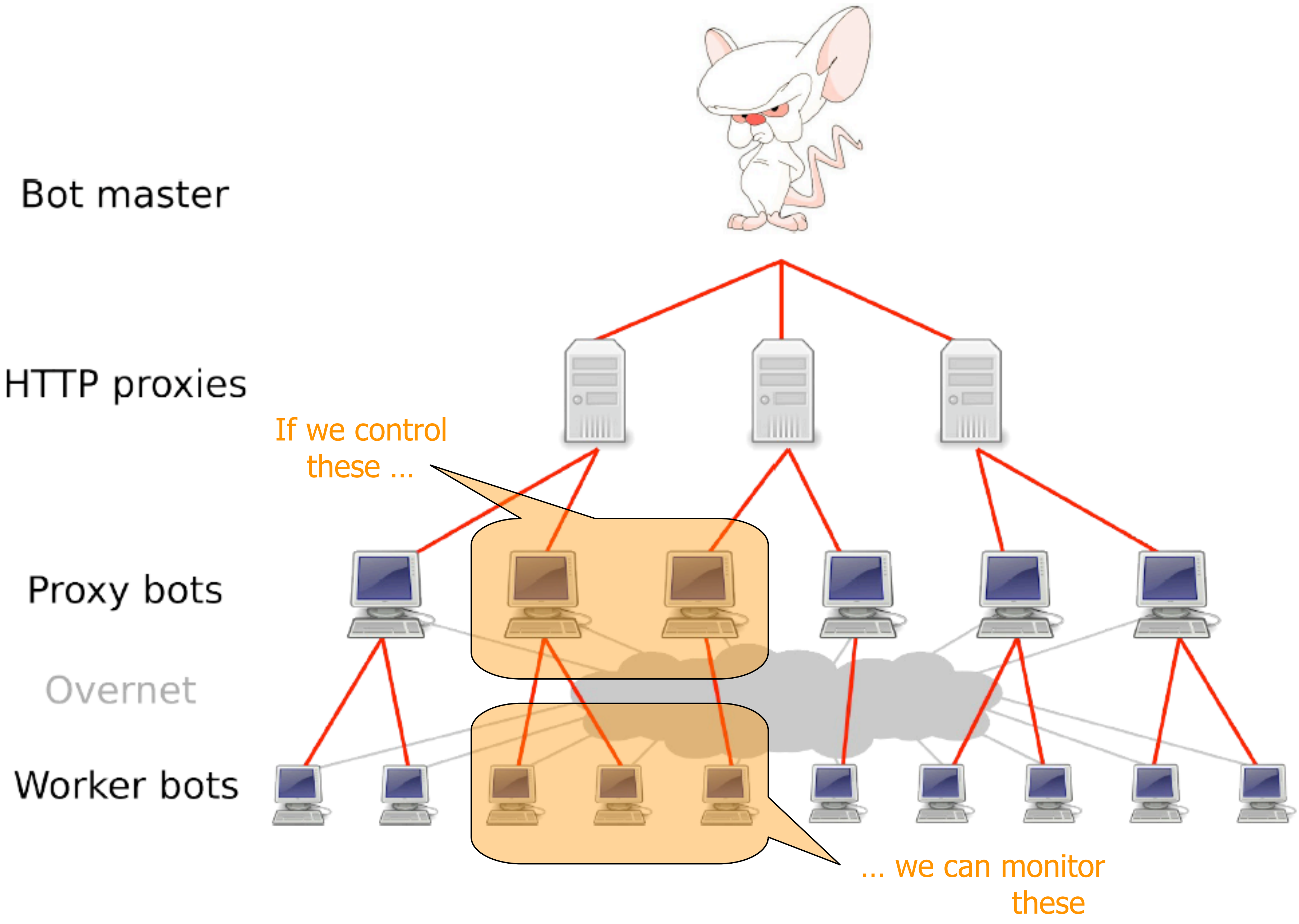


Individual counseling from $ 20. No Antenatal clinics :-)

GOOD DAY, GOOD MOOD AND GOOD BUSINESS [!]

CASH PARADISE UNIVERSITY ICQ: [redacted]
JABBER: [redacted]



Bot master

HTTP proxies

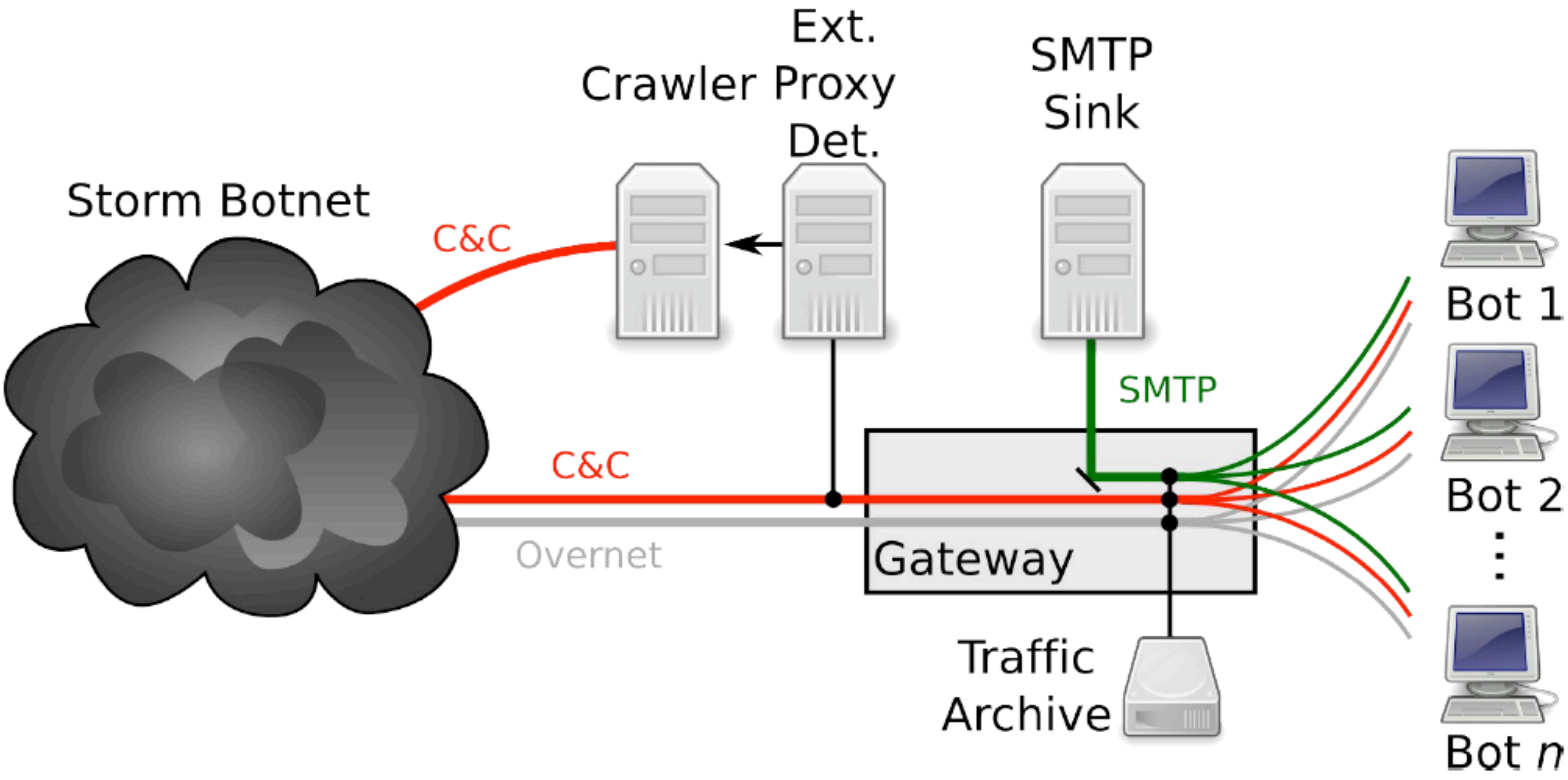
Proxy bots

Overnet

Worker bots

If we control
these …

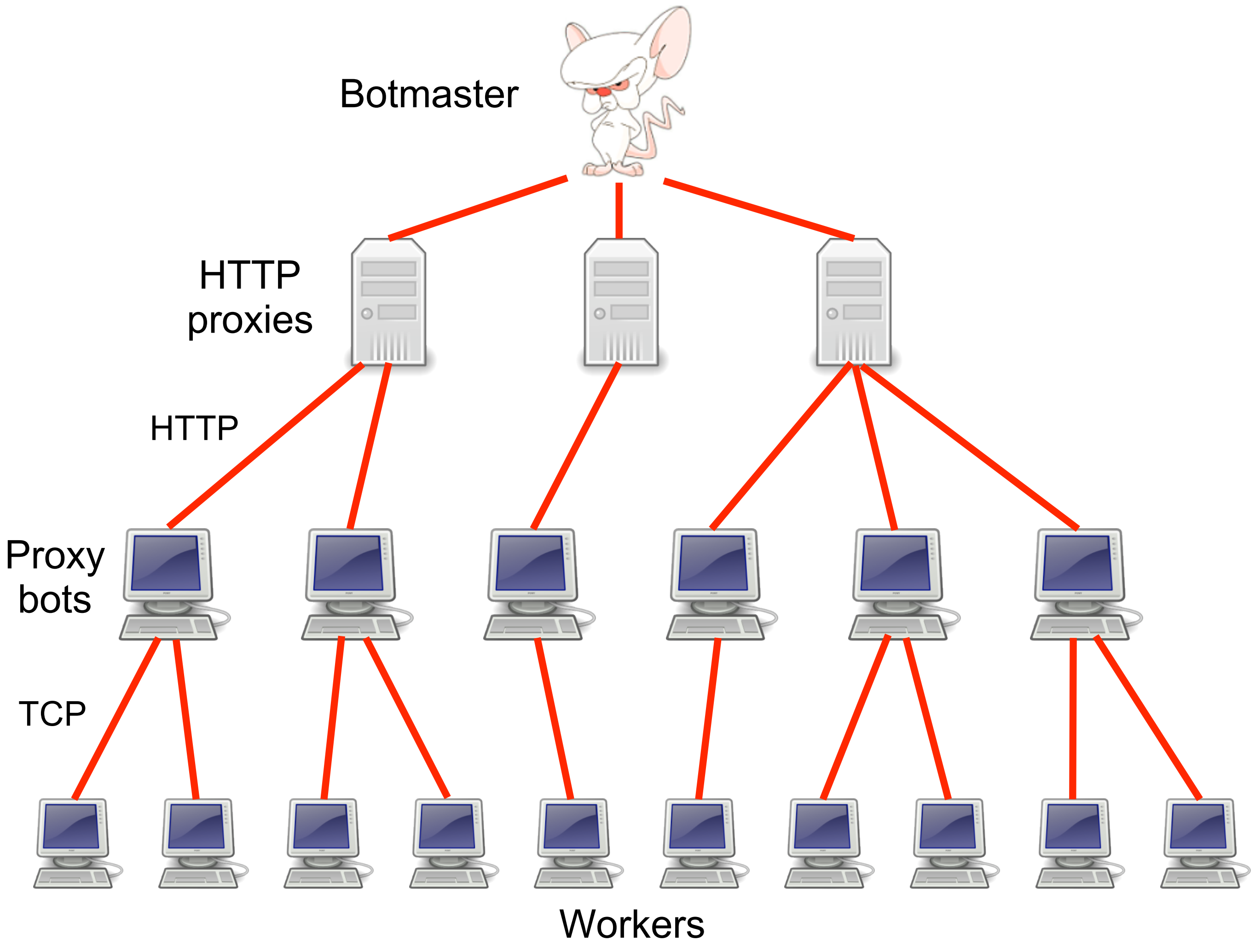
… we can monitor
these


Ext.
Crawler Proxy
Det.
SMTP
Sink
Storm Botnet
C&C
C&C
Overnet
SMTP
Gateway
Traffic
Archive
Bot 1
Bot 2
⋮
Bot *n*

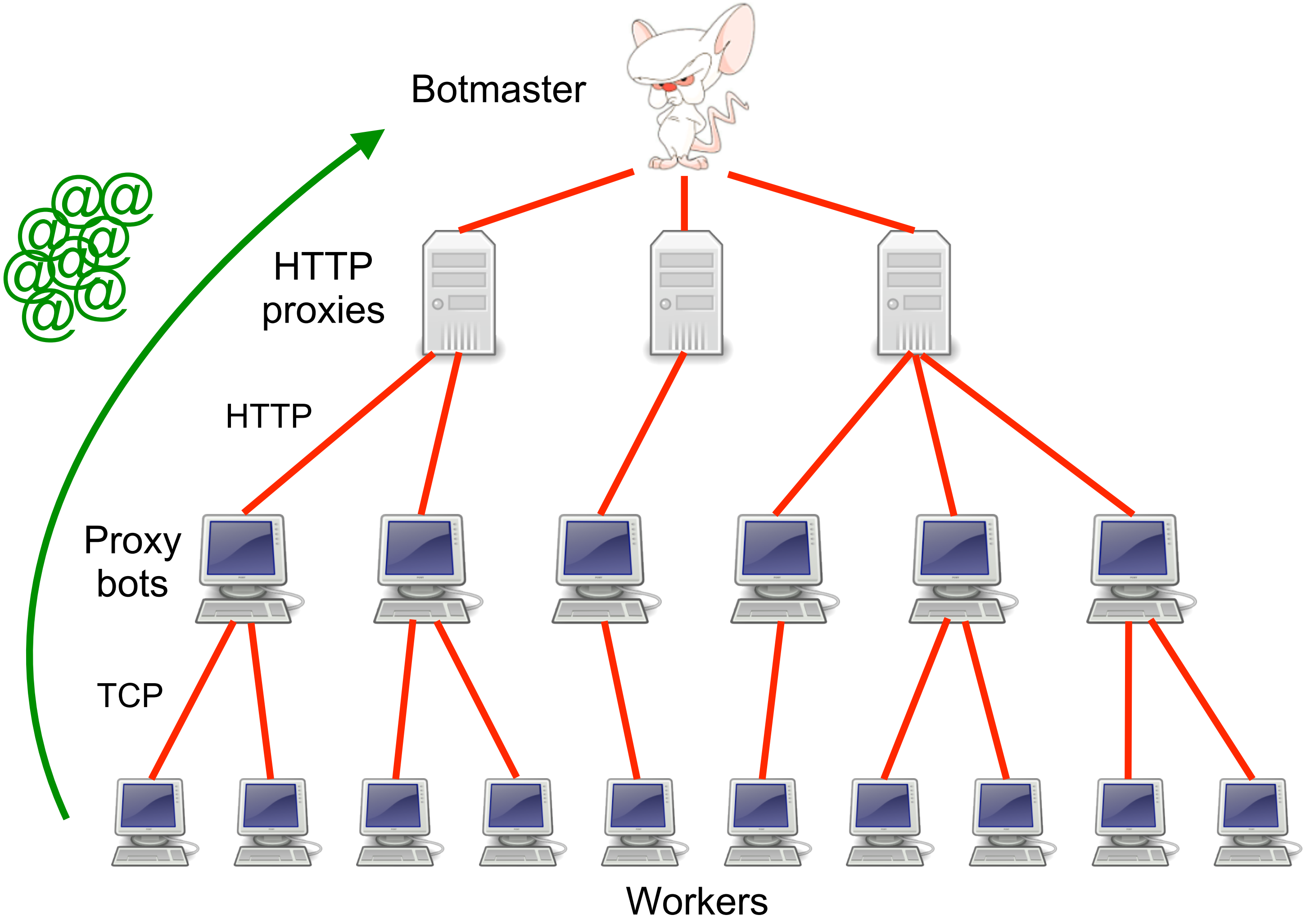
Types of Storm C&C Messages

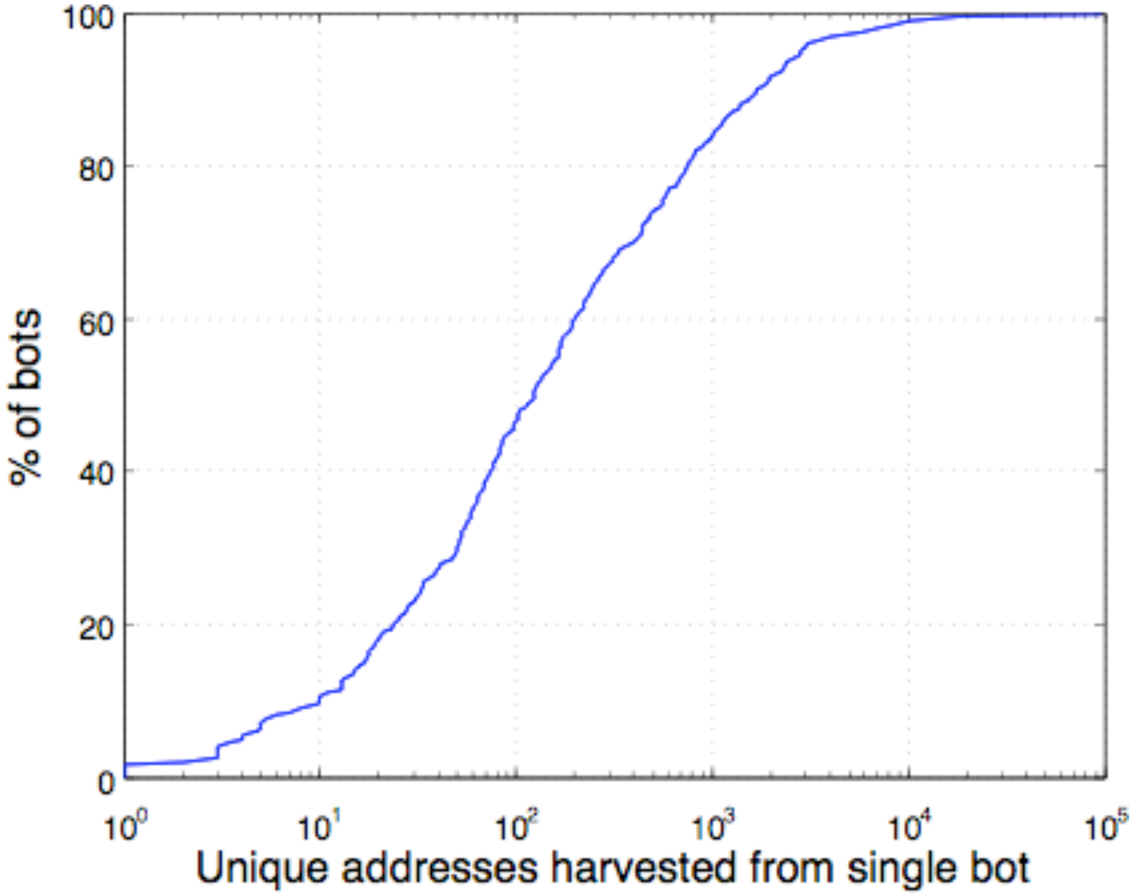
- Activation (report from bot to botmaster)
- Email address harvests
- Spamming instructions
- Delivery reports
- DDoS instructions
- FastFlux instructions
- HTTP proxy instructions
- Sniffed passwords report
- IFRAME injection/report

Spam campaign mechanics

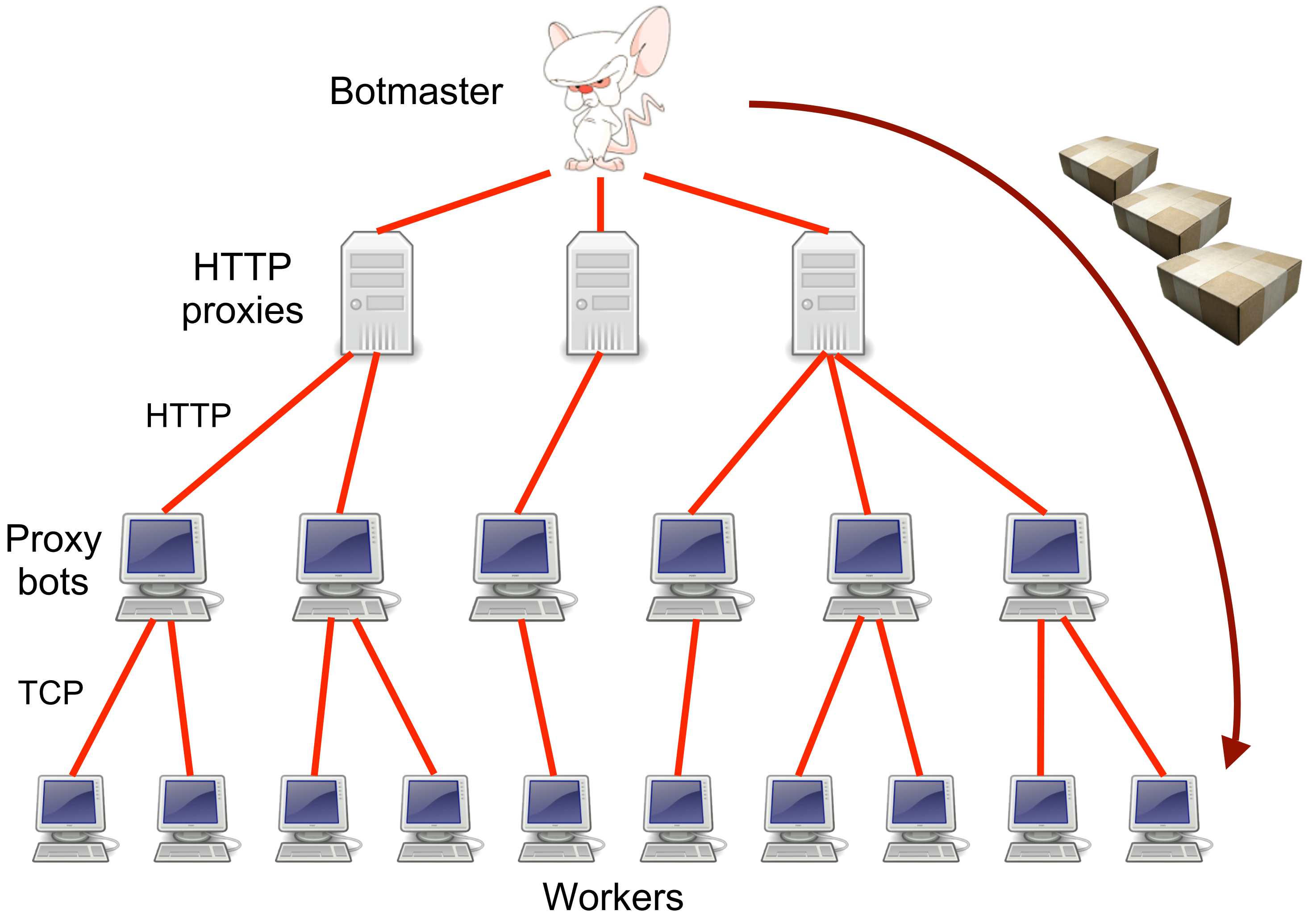


Campaign mechanics: harvest




100
80
60
40
20
0
% of bots
10^0
10^1
10^2
10^3
10^4
10^5
Unique addresses harvested from single bot

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.

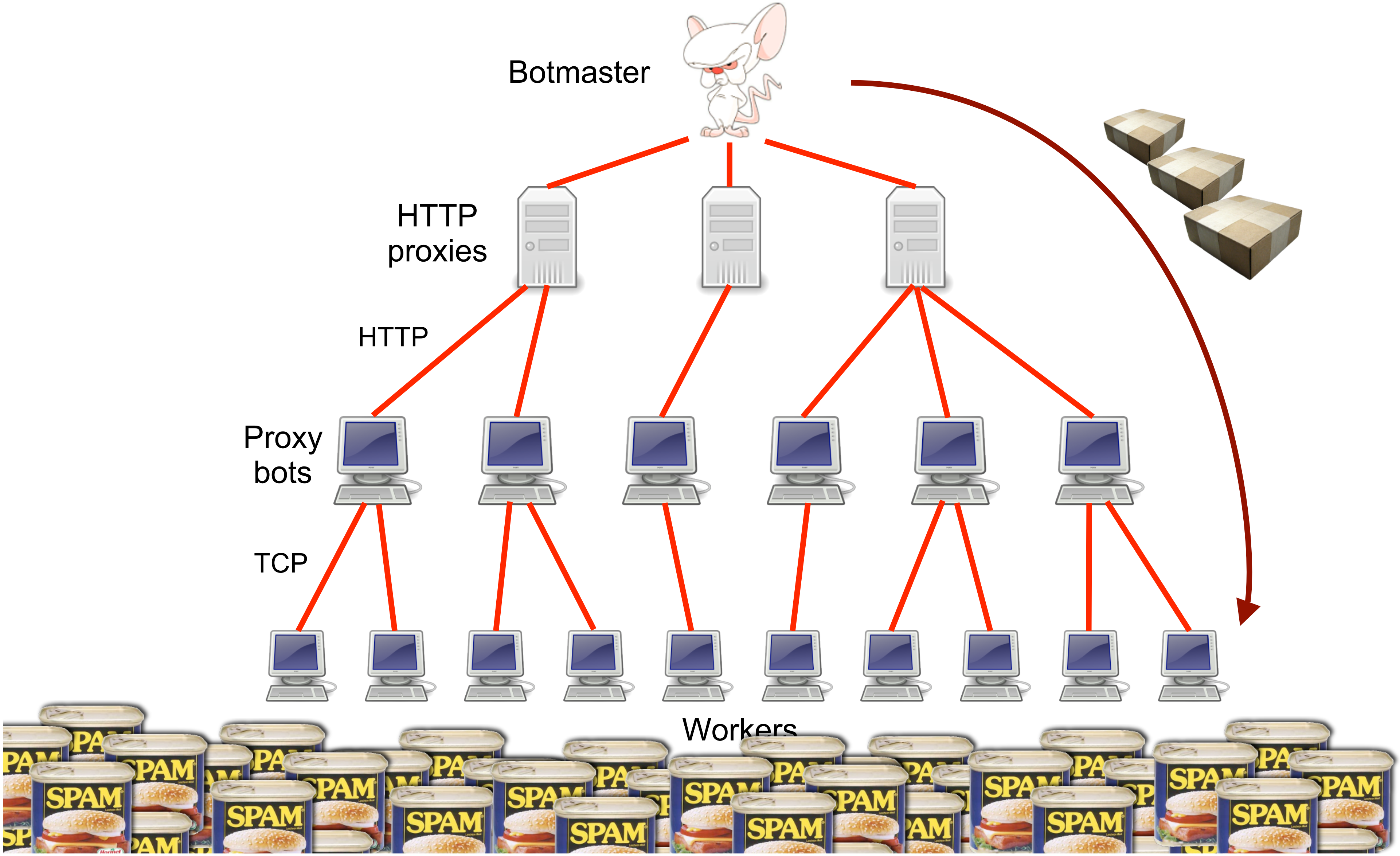
Table 2: Storm's spam-generation templating language.

```
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

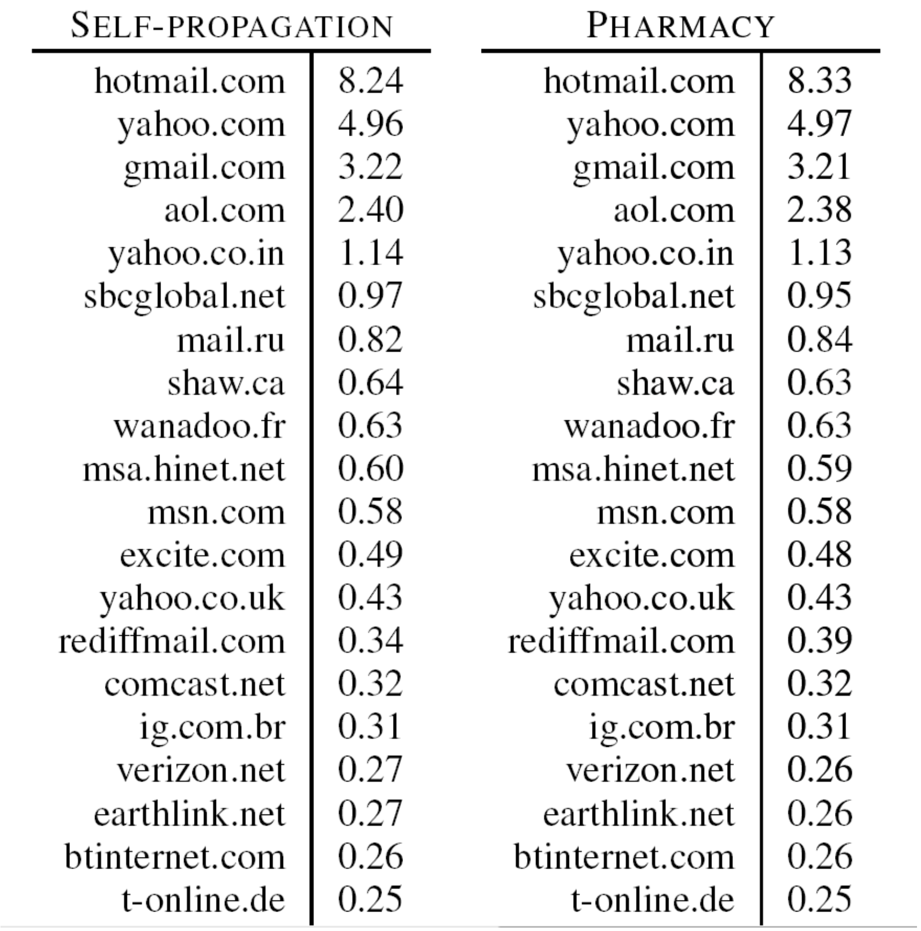


CLASS	DESCRIPTION
Money mule scam	Attemps to enroll the victim in money laundering schemes
Personal ad scam	Fake dating/matchmaking invitations intended to convince victim to advance money
Job ads	Variant of money-mule scams, new “employee” is asked to forward money or goods
Self-propagation	Tricks or lures victims into executing malicious binaries[1]
Phishing	Entices victims to enter sensitive information at fake bank sites or similars
Pharmaceutical	Pointers to web sites selling Viagra, Cialis, and other “male enhancement” products
Stock scam	Tries to convince victim to buy a particular stock suppsedly about to increase in value
Other ads	Other kinds of advertising
Image spam	Image-based spam[2]
Other	Broken or empty templates, noise-only templates, etc.[3]

Table 3: Meanings of campaign classes.

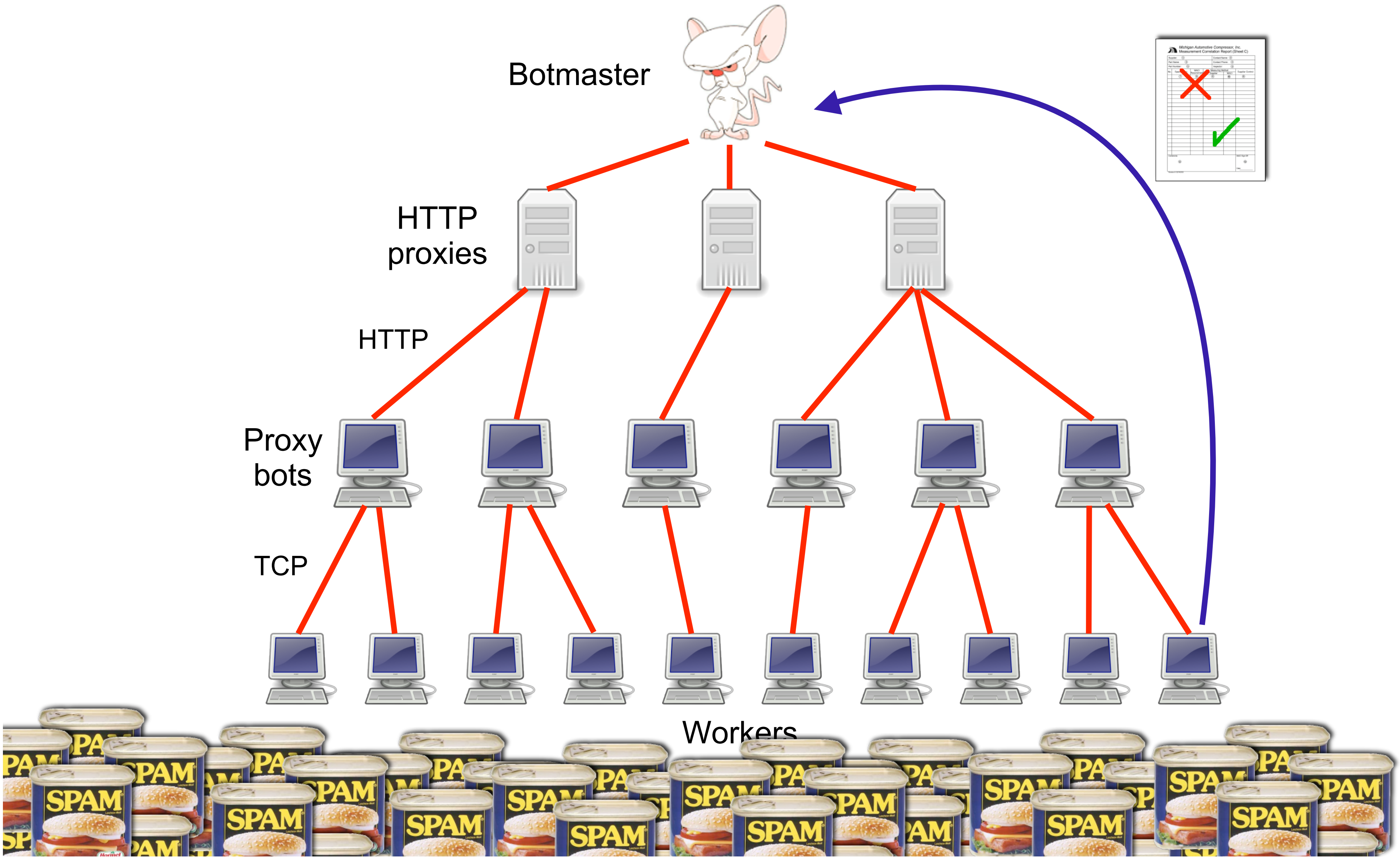
Who is targeted?

- Top 20 domains
  - Many Web mail & broadband providers, but very long tail
- Campaigns have nearly identical distributions
  - Same scammers, or target lists sold to multiple scammers
- Also see spam campaigns sent solely to *test accounts*

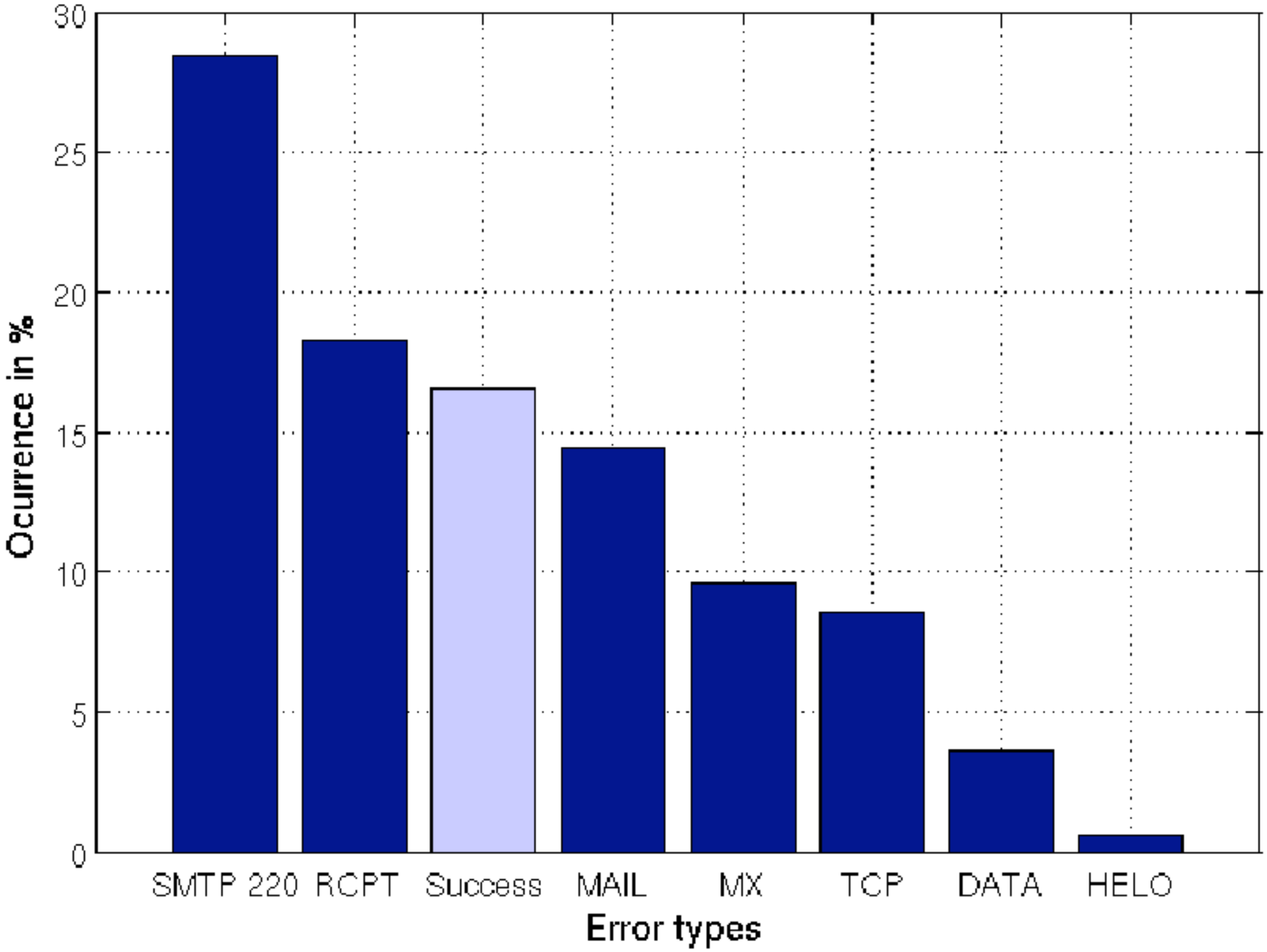


SELF-PROPAGATION		PHARMACY	
hotmail.com	8.24	hotmail.com	8.33
yahoo.com	4.96	yahoo.com	4.97
gmail.com	3.22	gmail.com	3.21
aol.com	2.40	aol.com	2.38
yahoo.co.in	1.14	yahoo.co.in	1.13
sbcglobal.net	0.97	sbcglobal.net	0.95
mail.ru	0.82	mail.ru	0.84
shaw.ca	0.64	shaw.ca	0.63
wanadoo.fr	0.63	wanadoo.fr	0.63
msa.hinet.net	0.60	msa.hinet.net	0.59
msn.com	0.58	msn.com	0.58
excite.com	0.49	excite.com	0.48
yahoo.co.uk	0.43	yahoo.co.uk	0.43
rediffmail.com	0.34	rediffmail.com	0.39
comcast.net	0.32	comcast.net	0.32
ig.com.br	0.31	ig.com.br	0.31
verizon.net	0.27	verizon.net	0.26
earthlink.net	0.27	earthlink.net	0.26
btinternet.com	0.26	btinternet.com	0.26
t-online.de	0.25	t-online.de	0.25

Campaign mechanics: reporting



Measurements: delivery efficacy



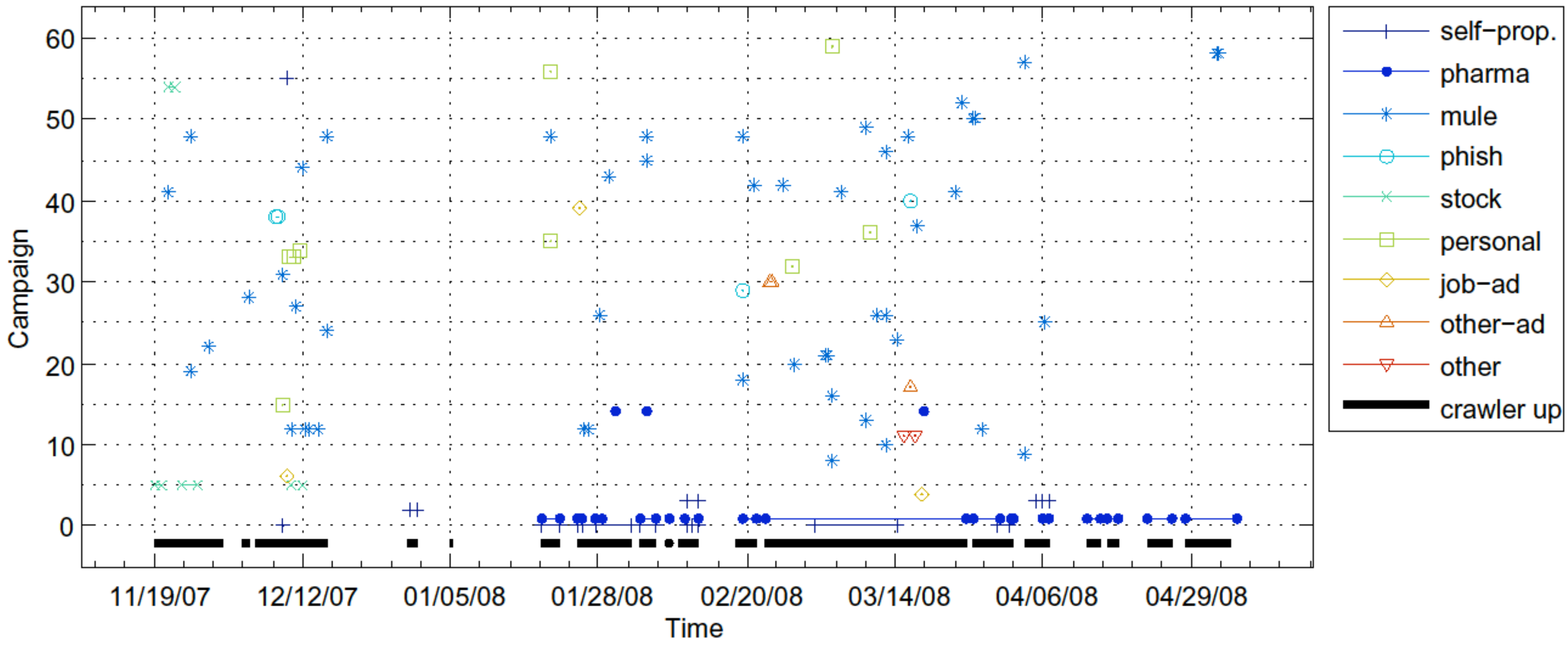
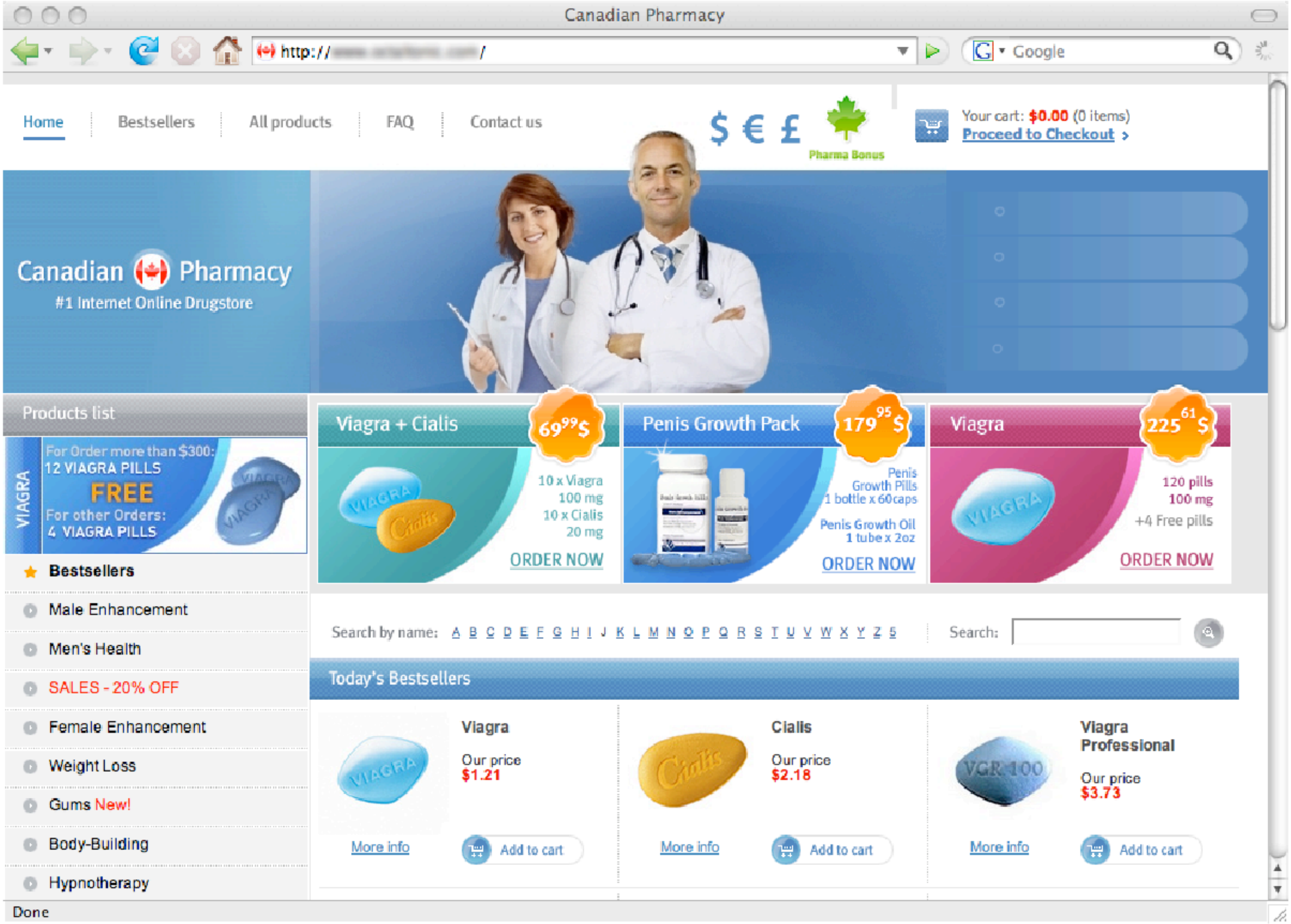


Figure 5: Classes and instances of spaming campaigns identified over time.



Canadian Pharmacy

http://[redacted]/

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

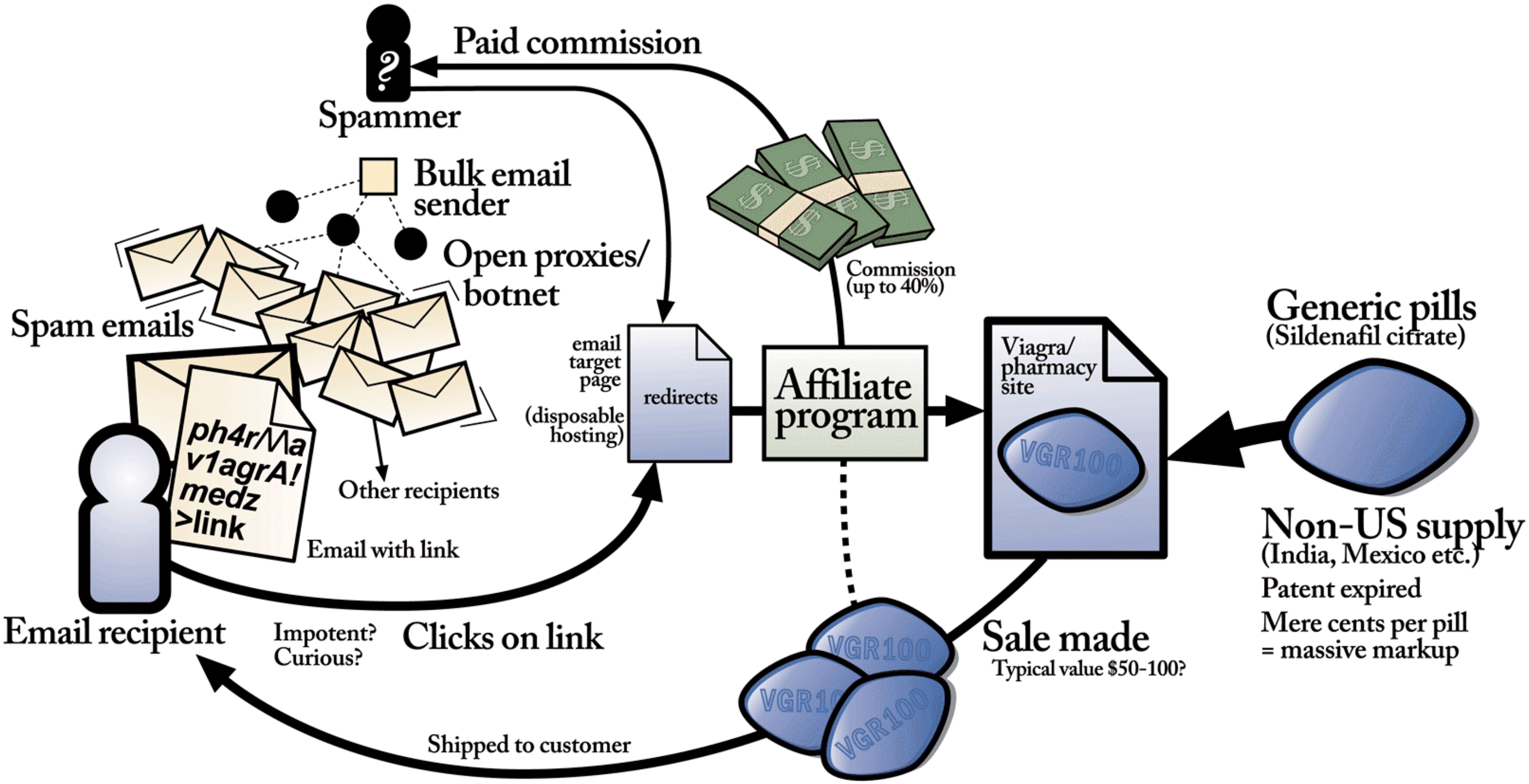
Search:

Today's Bestsellers

Viagra	Cialis	Viagra Professional
Our price $1.21	Our price $2.18	Our price $3.73
More info · Add to cart	More info · Add to cart	More info · Add to cart

Done

Anatomy of a modern Pharma spam campaign



Courtesy Stuart Brown
modernlifeisrubbish.co.uk

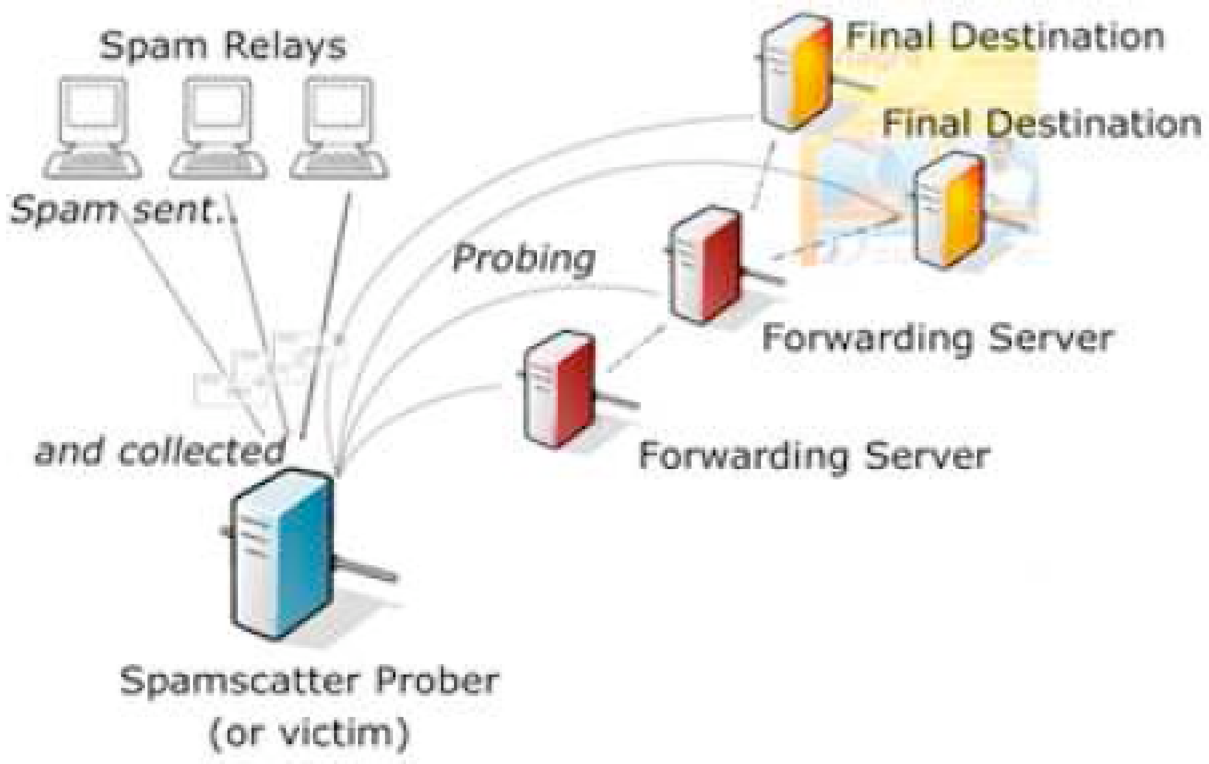


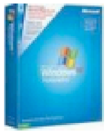
Figure 1: Components of a typical Internet scam.

Adobe Macromedia
Any-video-converter
apimac
app4mac
Apple Macintosh
Aquafadas
Avid
CD-DVD Software
code line
Creativebe
FabFilter
FileMaker
GAMES
Hardcoded Software
IK Multimedia
Intuit Quicken
Ironic
iSkysoft
JS8 Media
jumsoft
KavaSoft
Koingo
limit-point
Lynda Training
Mariner
Maxon Cinema for MAC
McAfee Anti-virus
mesadynamics
Metaobject
Microsoft for MAC
Native Instruments
Navicat
Office software
Other
Photo and Graphic Editors
positiveteam
publicspace
Quark XPress
Re:VisionEffects
realmacsoftware
red sweater
Rogue Amoeba
ronimusic
Roxio
Smileonmymac
thelittleappfactory
Topaz
Utilites and Programming
Video and Audio Editors
VMware
zapptek

Browse by Category

info / Buy / Upgrade

Windows XP Professional with Service Pack 3



Download Price:	$59.95
Retail Price:	$259.95
You Save:	$200

info / Buy / Upgrade

Word 2010 32-bit

Download Price:	$59.95
Retail Price:	$199.95
You Save:	$140

info / add

Word 2010 64-bit

Download Price:	$59.95
Retail Price:	$199.95
You Save:	$140

info / add

Excel 2010 32-bit

Download Price:	$59.95
Retail Price:	$199.95
You Save:	$140

info / add

Excel 2010 64-bit

Download Price:	$59.95
Retail Price:	$199.95
You Save:	$140

info / add

Retail Price:	$1899.95
You Save:	$1700

info / Buy / Upgrade

Adobe Creative Suite 5 Design Premium for MAC

Download Price:	$179.95
Retail Price:	$1899.95
You Save:	$1720

info / Buy / Upgrade

Adobe Photoshop CS5 Extended for MAC

Download Price:	$69.95
Retail Price:	$999.95
You Save:	$930

info / Buy / Upgrade

Adobe Photoshop Lightroom 3 for MAC

Download Price:	$69.95
Retail Price:	$299.95
You Save:	$230

info / Buy / Upgrade

Adobe Dreamweaver CS5 for MAC

Download Price:	$69.95
Retail Price:	$399.95
You Save:	$330

info / Buy / Upgrade

Adobe Creative Suite 4 Master Collection for MAC

Download Price:	$199.95
Retail Price:	$2599.95
You Save:	$2400

info / Buy / Upgrade

Windows Vista 32bit and Office 2010
Windows XP and Office 2007
Adobe PACK - 1
Mac Box Set

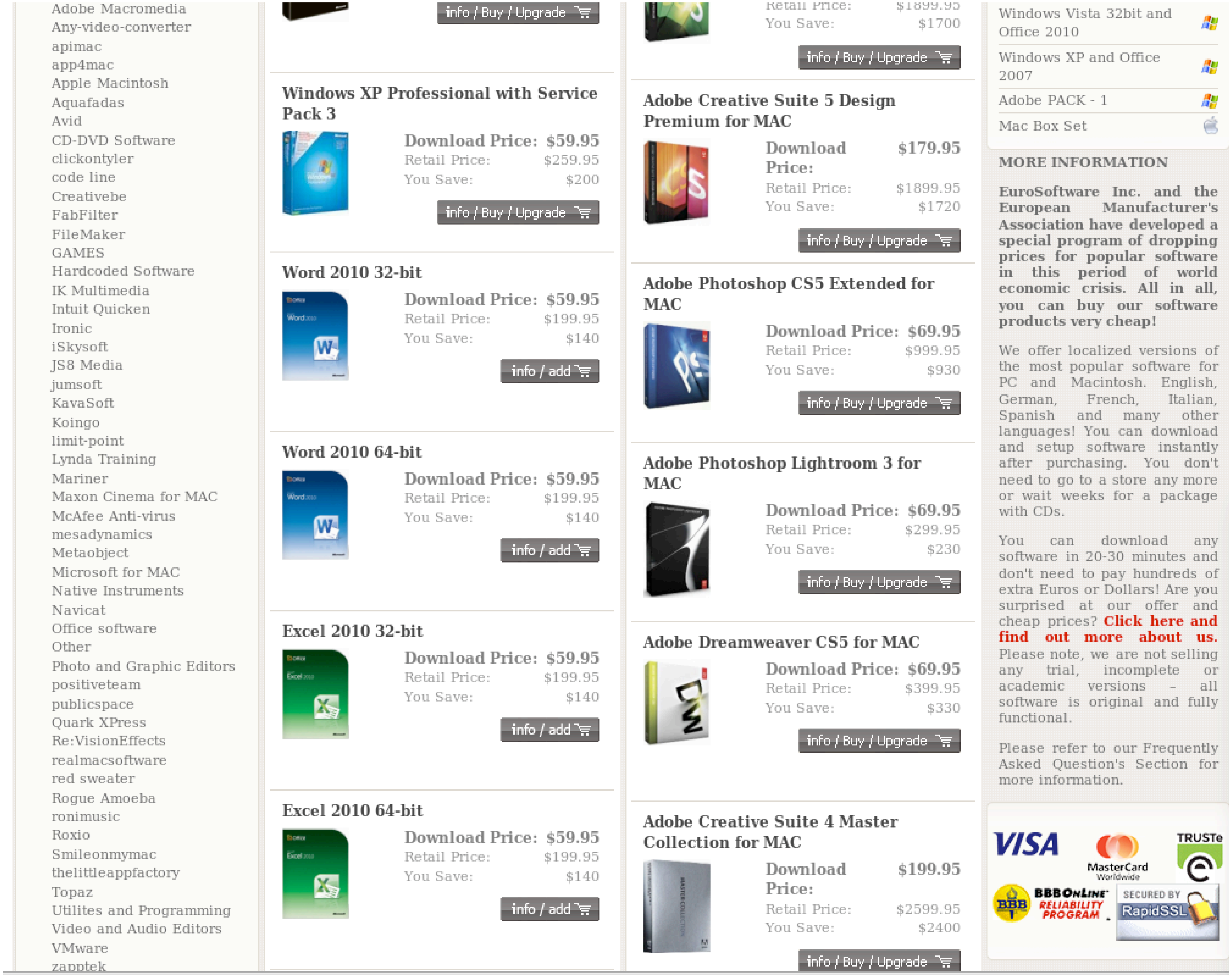
MORE INFORMATION

EuroSoftware Inc. and the European Manufacturer's Association have developed a special program of dropping prices for popular software in this period of world economic crisis. All in all, you can buy our software products very cheap!

We offer localized versions of the most popular software for PC and Macintosh. English, German, French, Italian, Spanish and many other languages! You can download and setup software instantly after purchasing. You don't need to go to a store any more or wait weeks for a package with CDs.

You can download any software in 20-30 minutes and don't need to pay hundreds of extra Euros or Dollars! Are you surprised at our offer and cheap prices? **Click here and find out more about us.** Please note, we are not selling any trial, incomplete or academic versions - all software is original and fully functional.

Please refer to our Frequently Asked Question's Section for more information.



Adobe Macromedia
Any-video-converter
apimac
app4mac
Apple Macintosh
Aquafadas
Avid
CD-DVD Software
clickontyler
code line
Creativebe
FabFilter
FileMaker
GAMES
Hardcoded Software
IK Multimedia
Intuit Quicken
Ironic
iSkysoft
JS8 Media
jumsoft
KavaSoft
Koingo
limit-point
Lynda Training
Mariner
Maxon Cinema for MAC
McAfee Anti-virus
mesadynamics
Metaobject
Microsoft for MAC
Native Instruments
Navicat
Office software
Other
Photo and Graphic Editors
positiveteam
publicspace
Quark XPress
Re:VisionEffects
realmacsoftware
red sweater
Rogue Amoeba
ronimusic
Roxio
Smileonmymac
thelittleappfactory
Topaz
Utilites and Programming
Video and Audio Editors
VMware
zapptek

info / Buy / Upgrade

Windows XP Professional with Service Pack 3

Download Price: $59.95
Retail Price: $259.95
You Save: $200

info / Buy / Upgrade

Word 2010 32-bit

Download Price: $59.95
Retail Price: $199.95
You Save: $140

info / add

Word 2010 64-bit

Download Price: $59.95
Retail Price: $199.95
You Save: $140

info / add

Excel 2010 32-bit

Download Price: $59.95
Retail Price: $199.95
You Save: $140

info / add

Excel 2010 64-bit

Download Price: $59.95
Retail Price: $199.95
You Save: $140

info / add

Retail Price: $1899.95
You Save: $1700

info / Buy / Upgrade

Adobe Creative Suite 5 Design Premium for MAC

Download Price: $179.95
Retail Price: $1899.95
You Save: $1720

info / Buy / Upgrade

Adobe Photoshop CS5 Extended for MAC

Download Price: $69.95
Retail Price: $999.95
You Save: $930

info / Buy / Upgrade

Adobe Photoshop Lightroom 3 for MAC

Download Price: $69.95
Retail Price: $299.95
You Save: $230

info / Buy / Upgrade

Adobe Dreamweaver CS5 for MAC

Download Price: $69.95
Retail Price: $399.95
You Save: $330

info / Buy / Upgrade

Adobe Creative Suite 4 Master Collection for MAC

Download Price: $199.95
Retail Price: $2599.95
You Save: $2400

info / Buy / Upgrade

Windows Vista 32bit and Office 2010
Windows XP and Office 2007
Adobe PACK - 1
Mac Box Set

MORE INFORMATION

EuroSoftware Inc. and the European Manufacturer's Association have developed a special program of dropping prices for popular software in this period of world economic crisis. All in all, you can buy our software products very cheap!

We offer localized versions of the most popular software for PC and Macintosh. English, German, French, Italian, Spanish and many other languages! You can download and setup software instantly after purchasing. You don't need to go to a store any more or wait weeks for a package with CDs.

You can download any software in 20-30 minutes and don't need to pay hundreds of extra Euros or Dollars! Are you surprised at our offer and cheap prices? **Click here and find out more about us.** Please note, we are not selling any trial, incomplete or academic versions - all software is original and fully functional.

Please refer to our Frequently Asked Question's Section for more information.

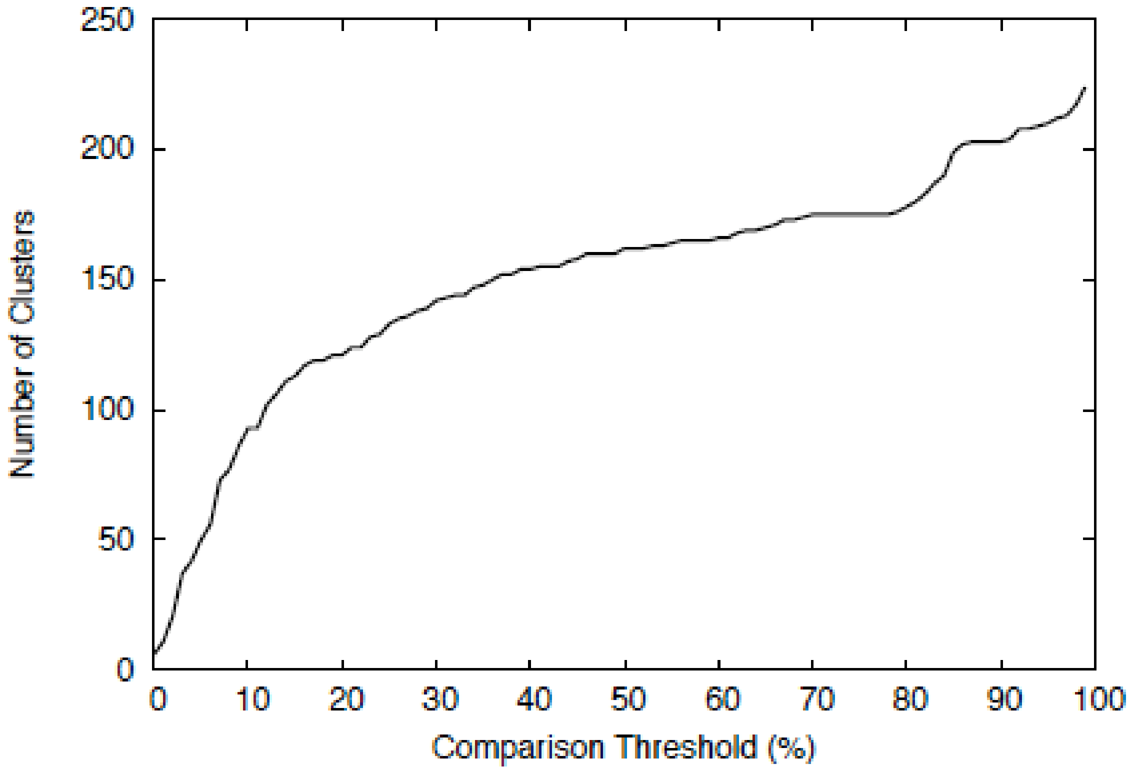
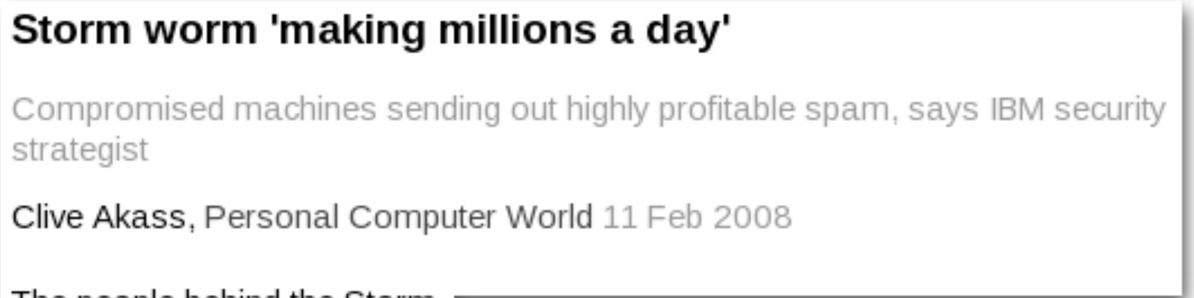


Figure 4: The choice of a threshold value for image shingling determines the number of clusters.

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.

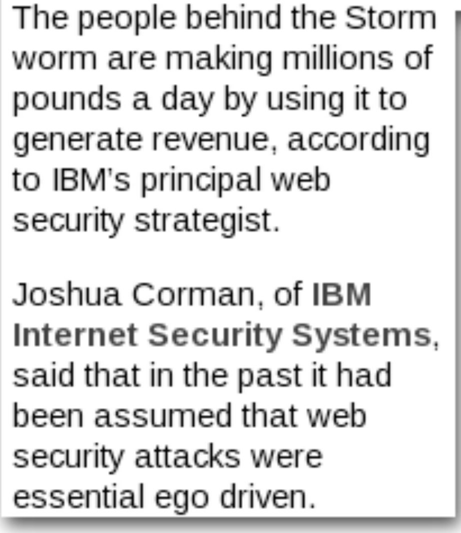
Are Bots & Spam the New Black Gold?



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

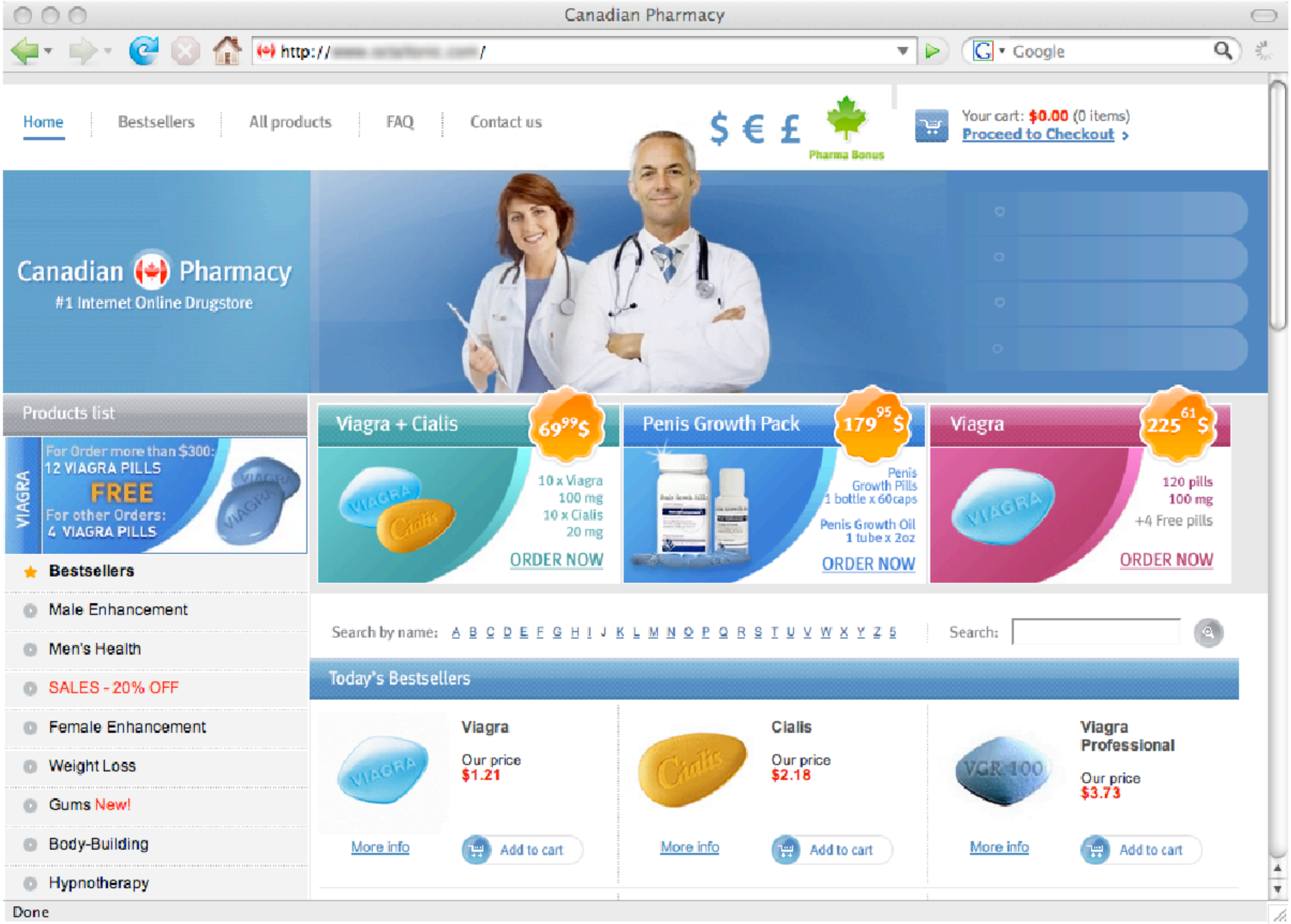


The people behind the Storm worm are making millions of pounds a day by using it to generate revenue, according to IBM's principal web security strategist.

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*



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

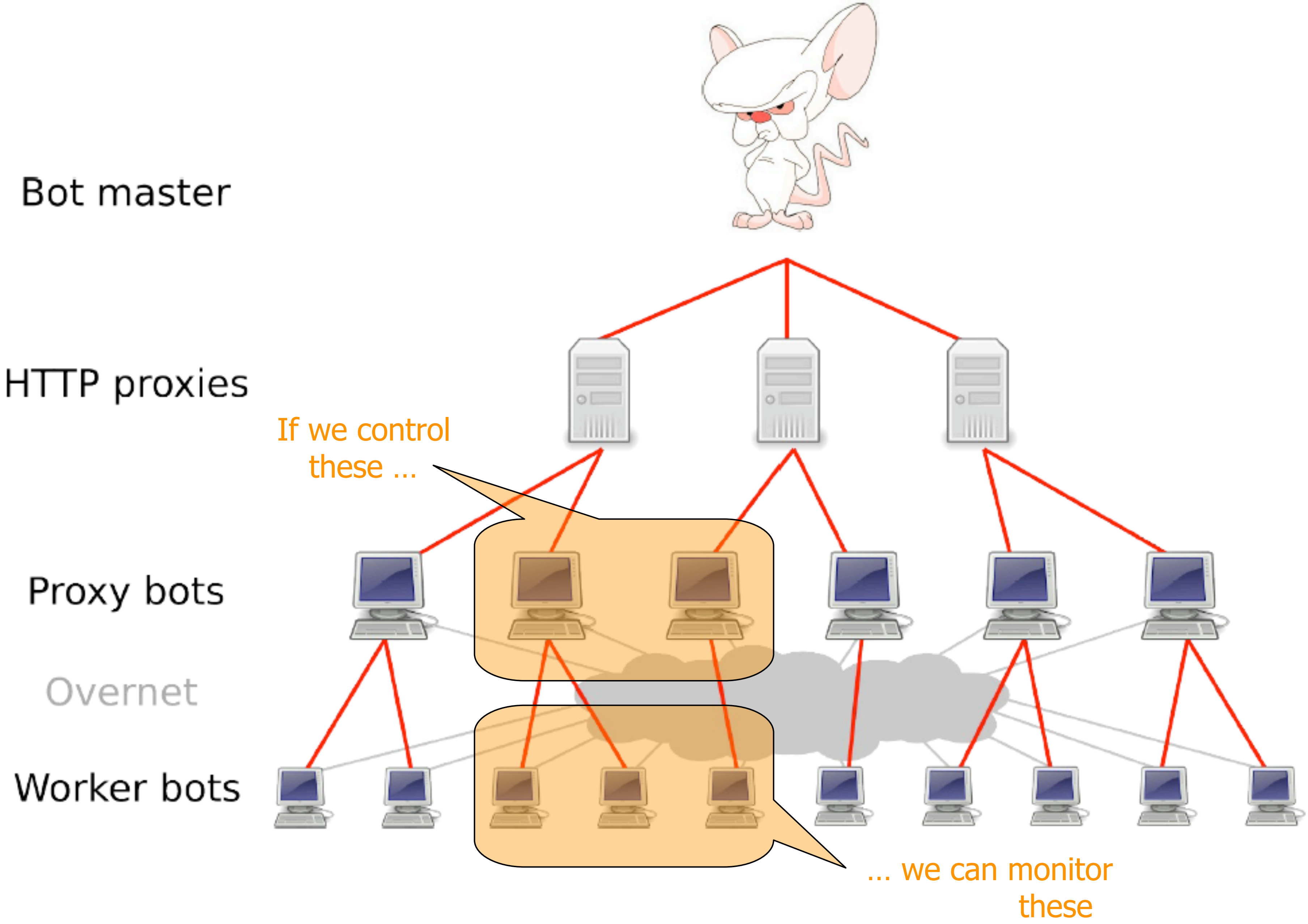
Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 5

Search:

Today's Bestsellers

Viagra	Cialis	Viagra Professional
Our price $1.21	Our price $2.18	Our price $3.73
More info Add to cart	More info Add to cart	More info Add to cart

Done



Bot master

HTTP proxies

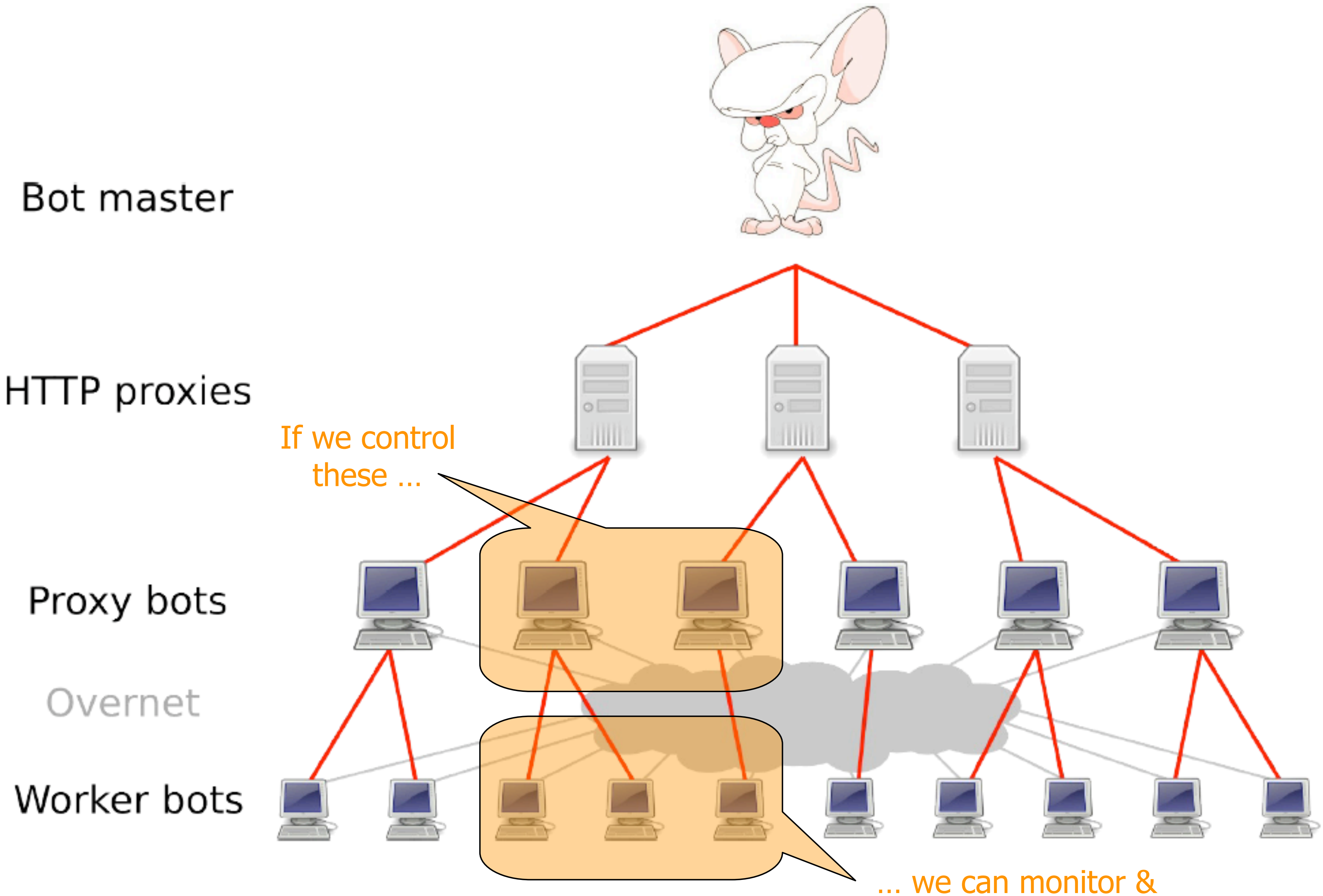
Proxy bots

Overnet

Worker bots

If we control these …

… we can monitor these



Bot master

HTTP proxies

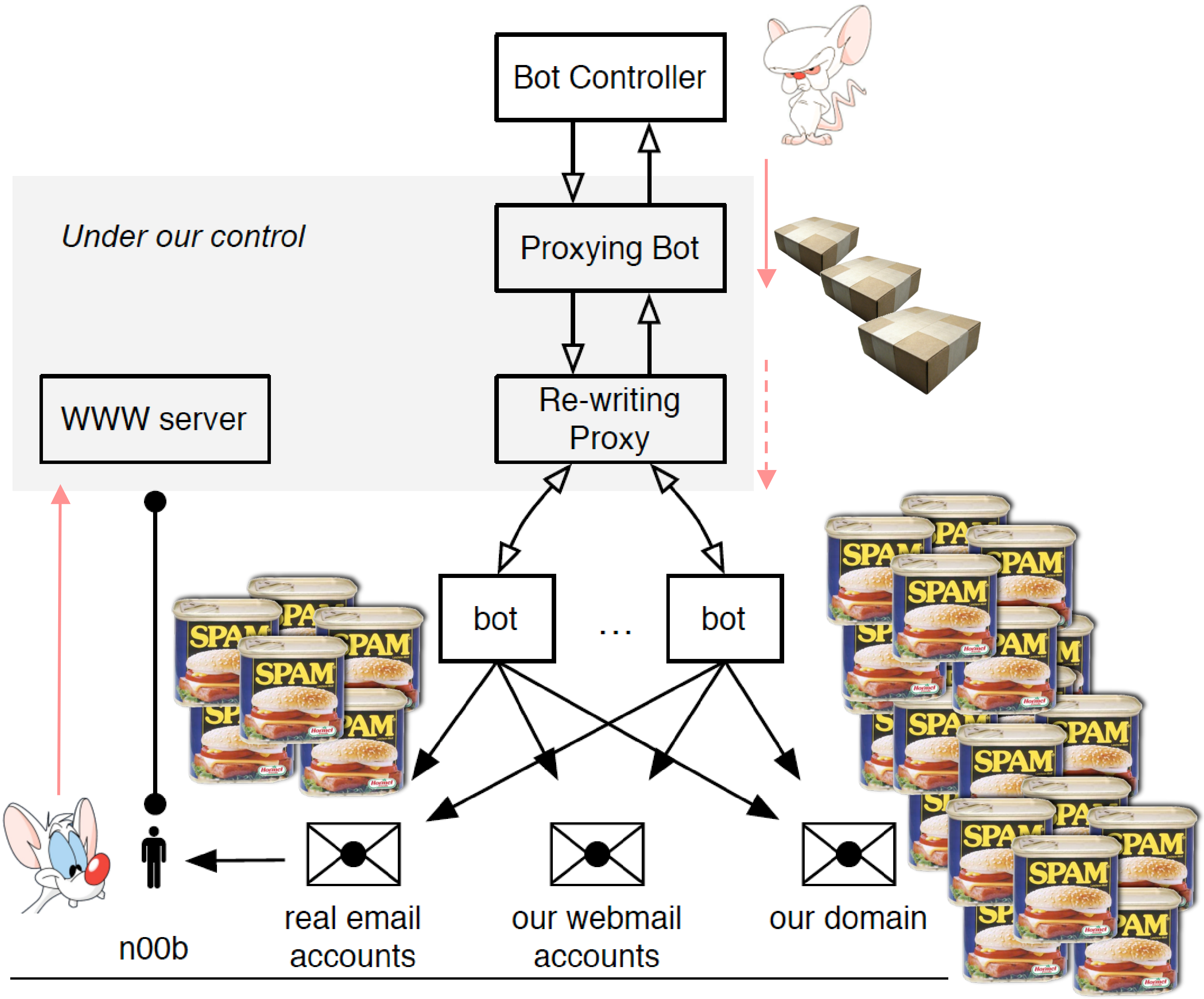
Proxy bots

Overnet

Worker bots

If we control these …

… we can monitor & **influence** these



Bot Controller

Proxying Bot

Re-writing Proxy

Under our control

WWW server

bot

…

bot

n00b

real email accounts

our webmail accounts

our domain

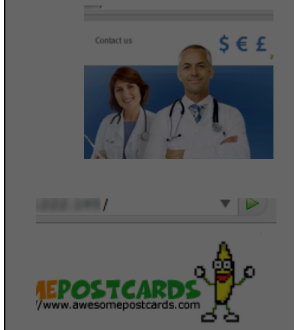
Spam conversion experiment

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

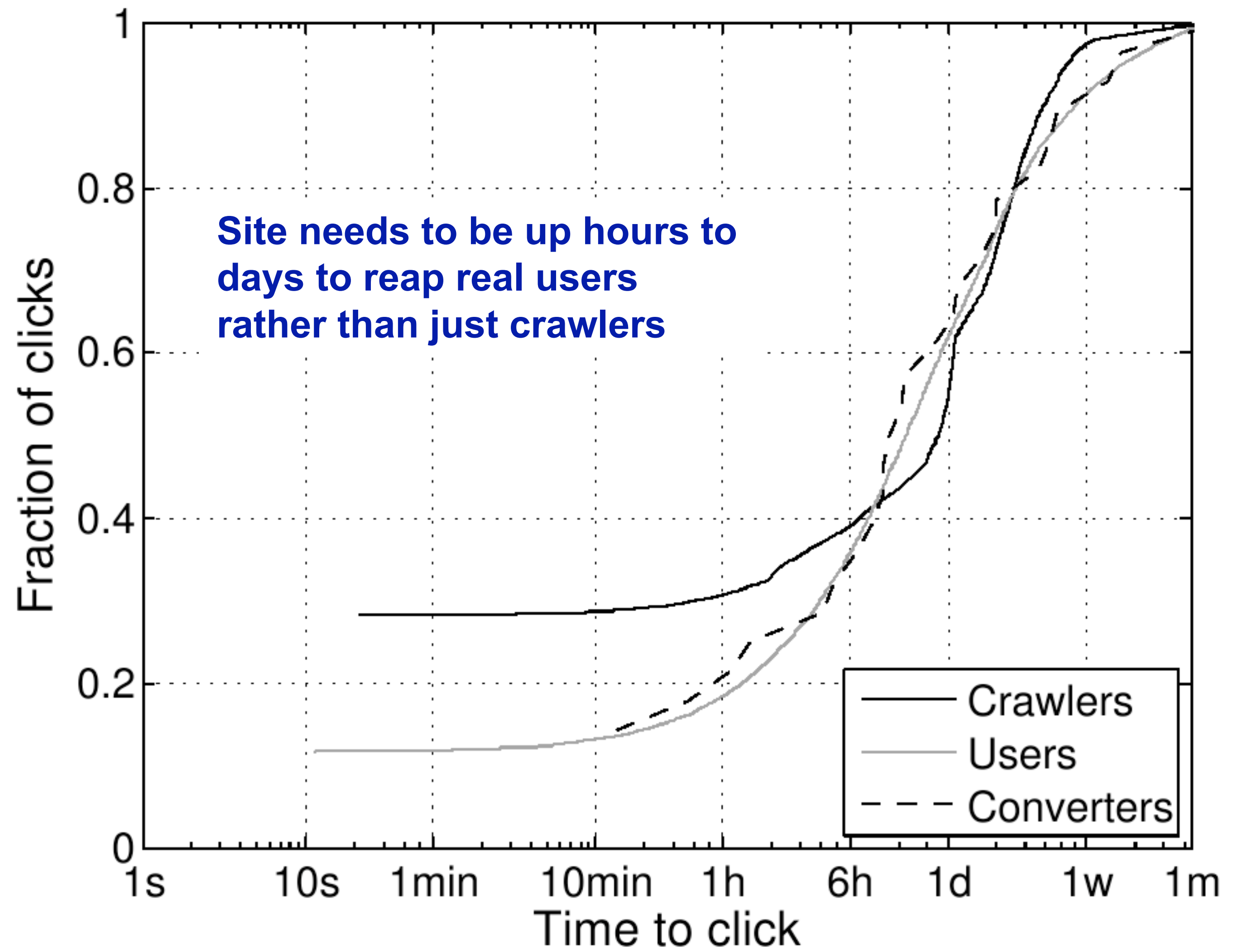
	Pharmacy Campaign	**E-card Campaigns**	
		Postcard	April Fool
Worker bots	31,348	17,639	3,678
Emails	347,590,389	83,665,479	38,651,124
Duration	19 days	7 days	3 days

Spa

Response rates by country



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



Site needs to be up hours to days to reap real users rather than just crawlers

Response Rate for Self−prop Email

Delivery Rate Prior to Blacklisting

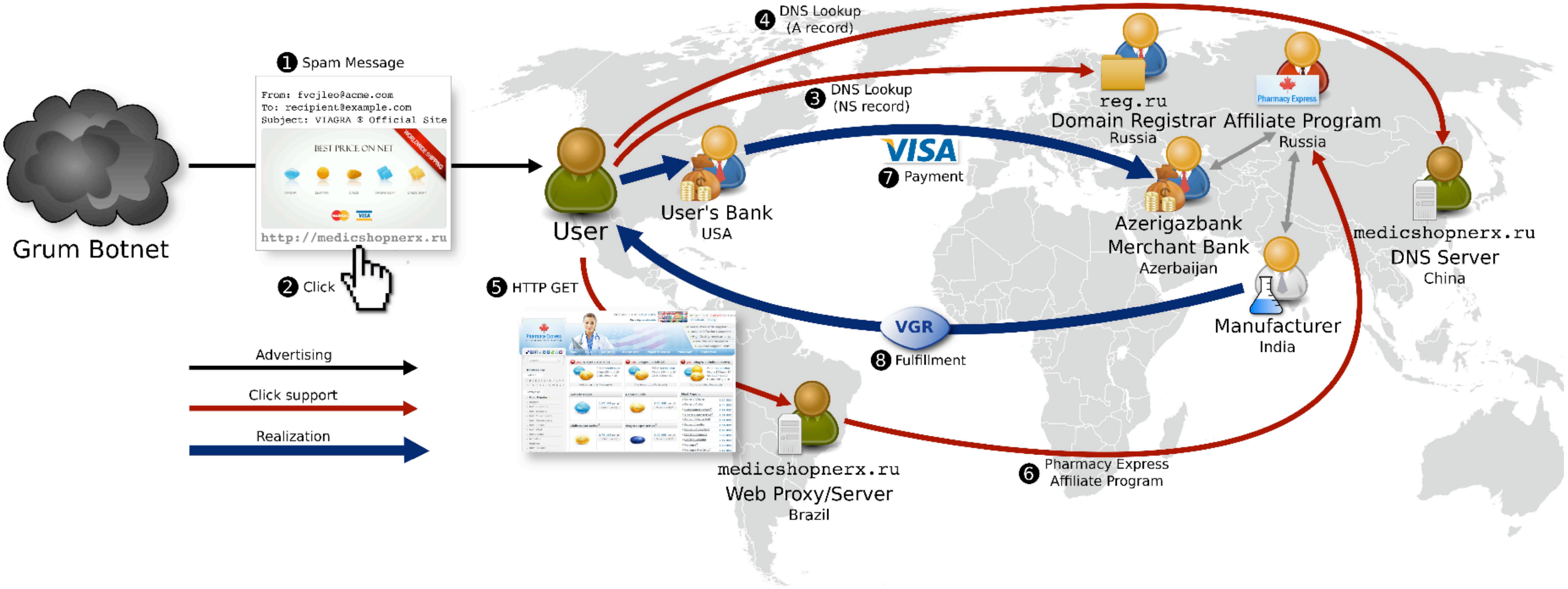
sions

0008%)

037%)

056%)

targeted


Grum Botnet
1 Spam Message
From: fvcjleo@acme.com
To: recipient@example.com
Subject: VIAGRA ® Official Site
BEST PRICE ON NET
http://medicshopnerx.ru
2 Click
User
5 HTTP GET
User's Bank
USA
4 DNS Lookup
(A record)
3 DNS Lookup
(NS record)
VISA
7 Payment
reg.ru
Domain Registrar
Russia
Pharmacy Express
Affiliate Program
Russia
Azerigazbank
Merchant Bank
Azerbaijan
medicshopnerx.ru
DNS Server
China
Manufacturer
India
VGR
8 Fulfillment
medicshopnerx.ru
Web Proxy/Server
Brazil
6 Pharmacy Express
Affiliate Program
Advertising
Click support
Realization

Feed	*Type*	*Received URLs*
Feed A	MX honeypot	32,548,304
Feed B	Seeded honey accounts	73,614,895
Feed C	MX honeypot	451,603,575
Feed D	Seeded honey accounts	30,991,248
Feed X	MX honeypot	198,871,030
Feed Y	Human identified	10,733,231
Feed Z	MX honeypot	12,517,244
Cutwail	Bot	3,267,575
Grum	Bot	11,920,449
MegaD	Bot	1,221,253
Rustock	Bot	141,621,731
Other bots	Bot	7,768
Total		968,918,303

Table I: Feeds of spam-advertised URLs used in this study. We collected feed data from August 1, 2010 through October 31, 2010.

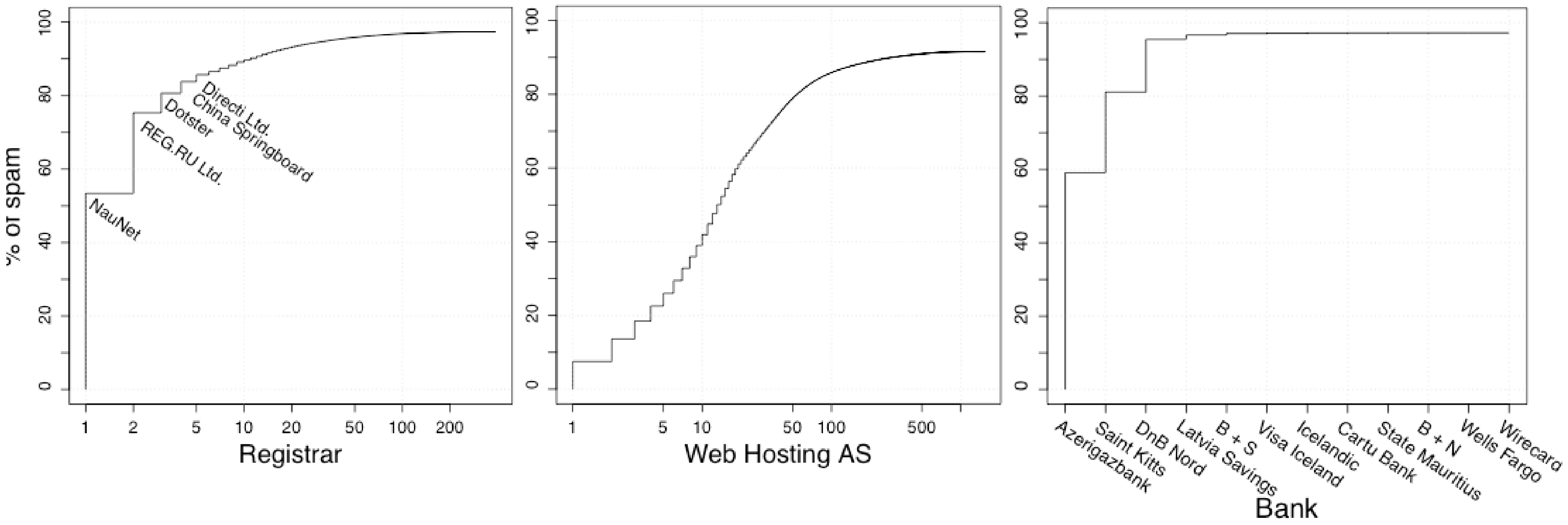


Figure 3: Takedown effectiveness when considering domain registrars (left), web hosters (center) and banks (right).