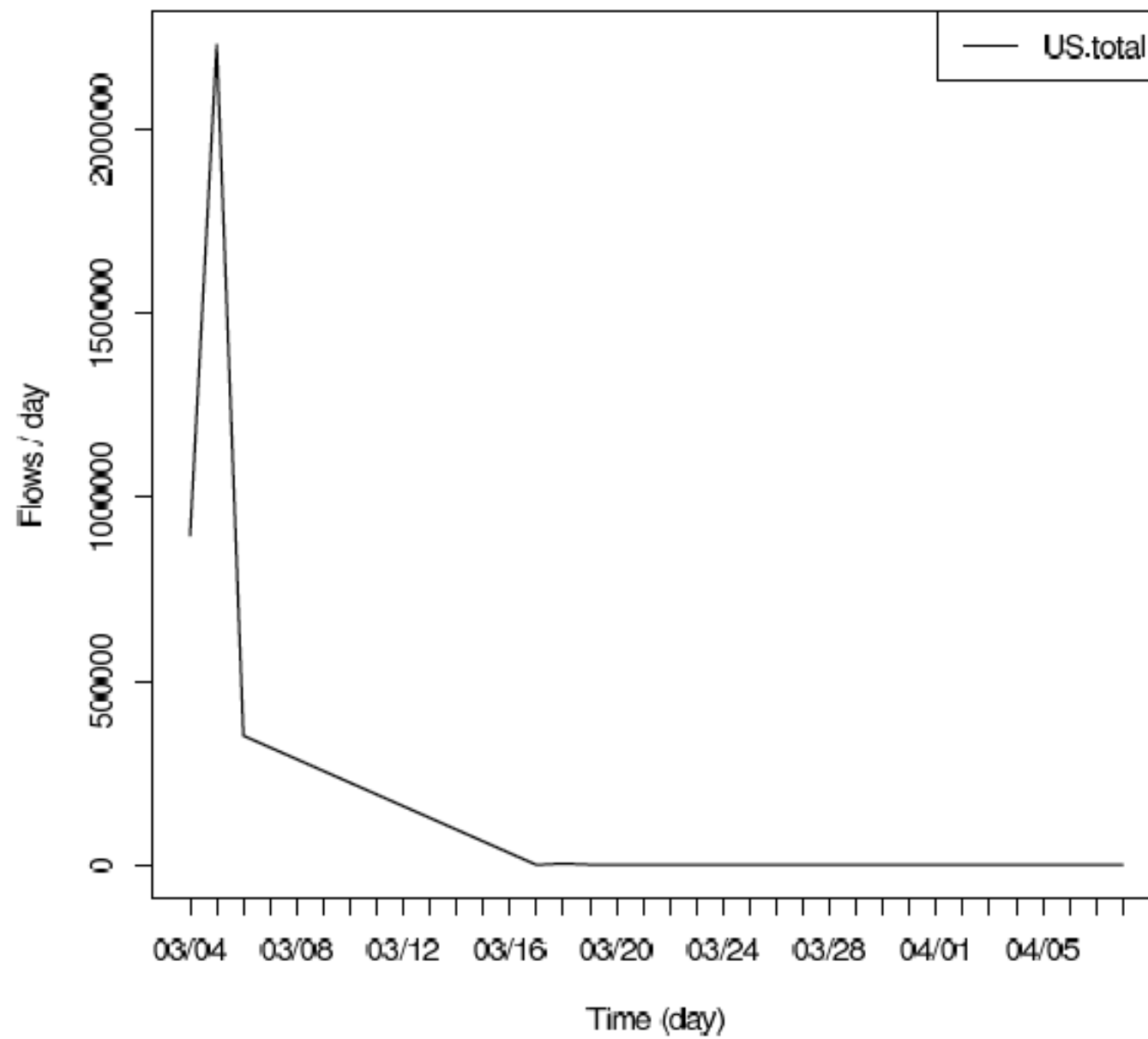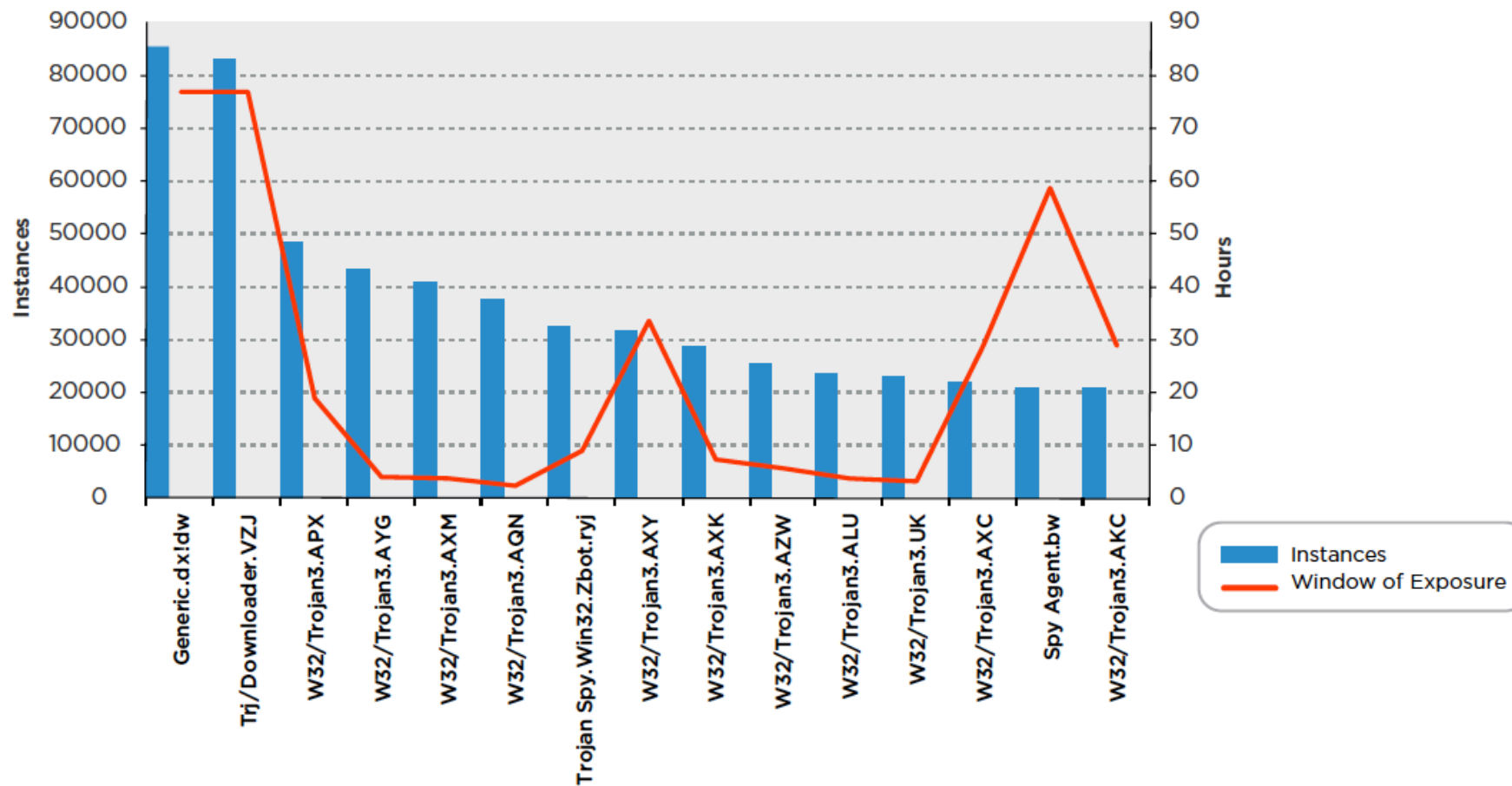(a) Presence of violations
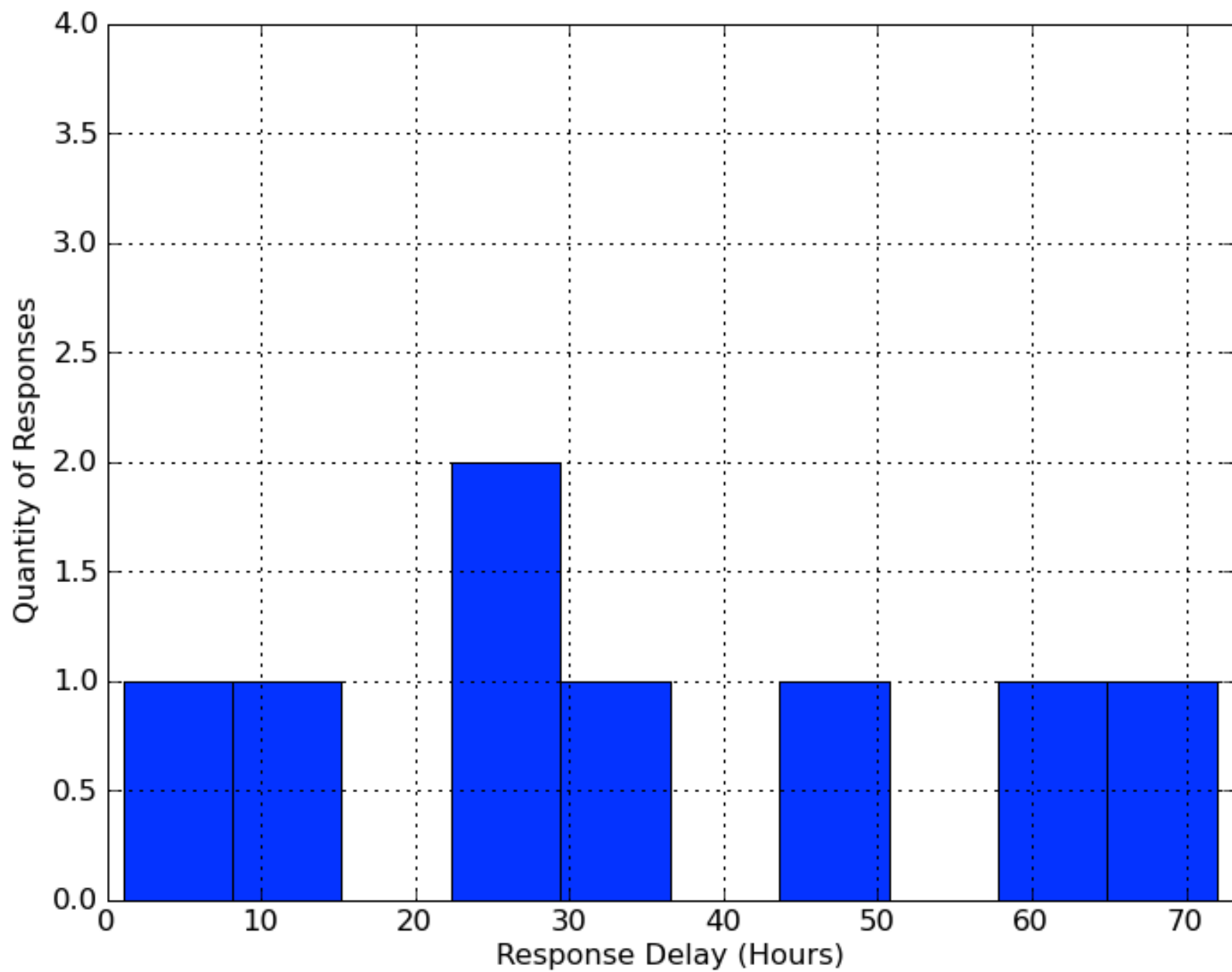
(b) Total traffic for `62.34.164.84`.

AV Vendor Confirmed ThreatSeeker Catches

Jan 2009 - Jun 2009

Categories (x-axis):
Generic.dx!dw, Trj/Downloader.VZJ, W32/Trojan3.APX, W32/Trojan3.AYG, W32/Trojan3.AXM, W32/Trojan3.AQN, Trojan Spy.Win32.Zbot.ryj, W32/Trojan3.AXY, W32/Trojan3.AXK, W32/Trojan3.AZW, W32/Trojan3.ALU, W32/Trojan3.UK, W32/Trojan3.AXC, Spy Agent.bw, W32/Trojan3.AKC

Legend:
Instances
Window of Exposure

Percentage of Global Spam - Classified as Spam or Containing Virus

Month	Percentage Spam	Percentage Virus
Jun-09	87.5	0.7
May-09	88.1	0.1
Apr-09	87.2	0.1
Mar-09	87.2	0.1
Feb-09	88.3	0.1
Jan-09	87.9	0.2

Legend:
- Percentage Spam
- Percentage Virus

X-axis: 86.5%, 87%, 87.5%, 88%, 88.5%
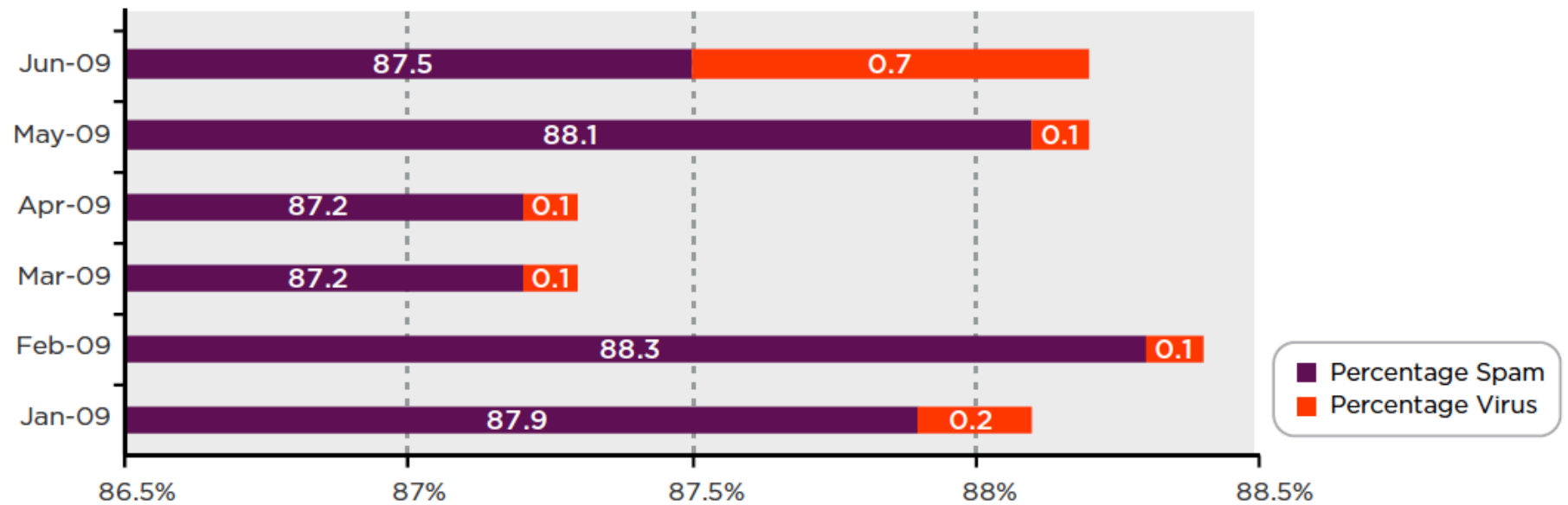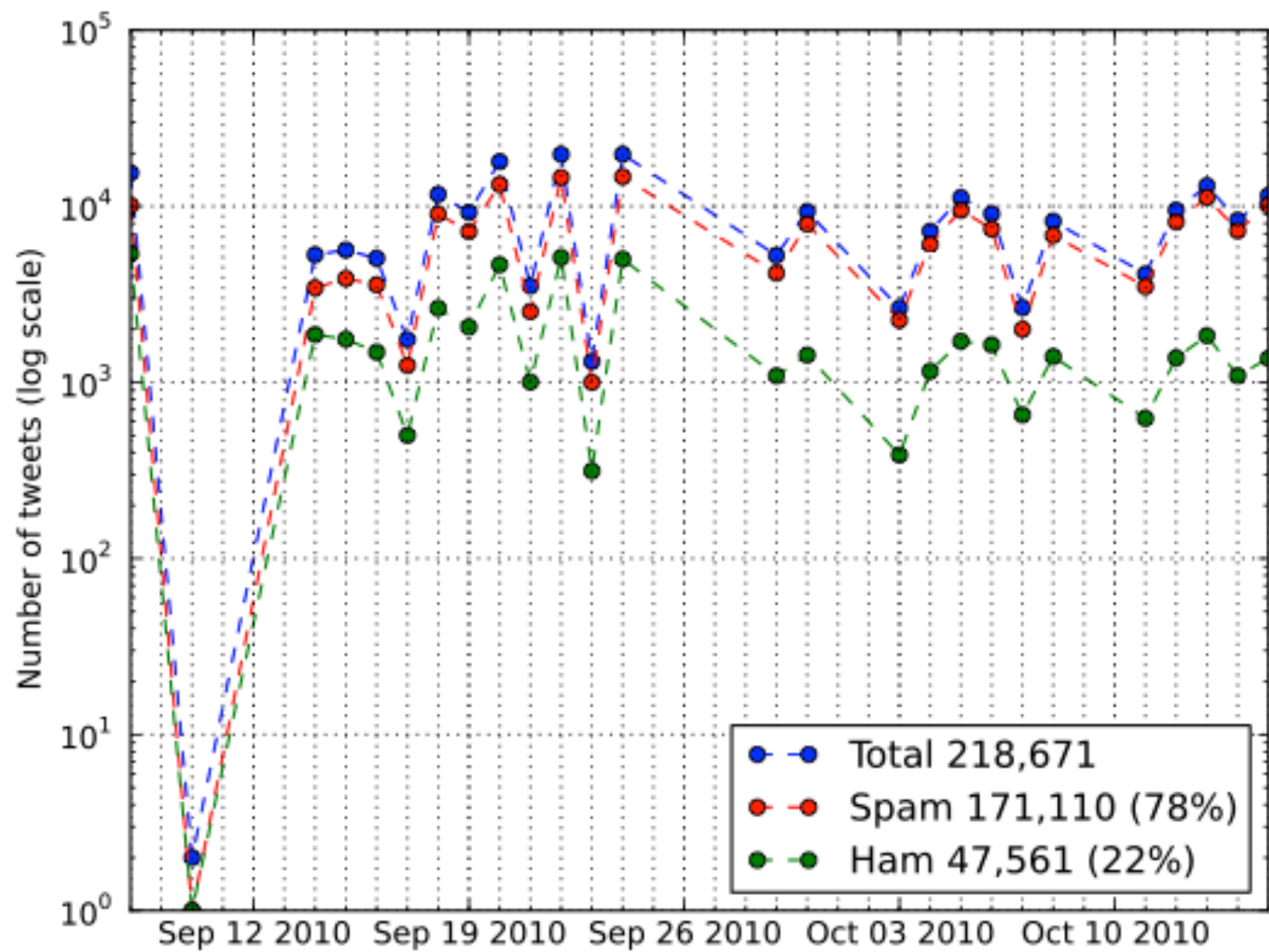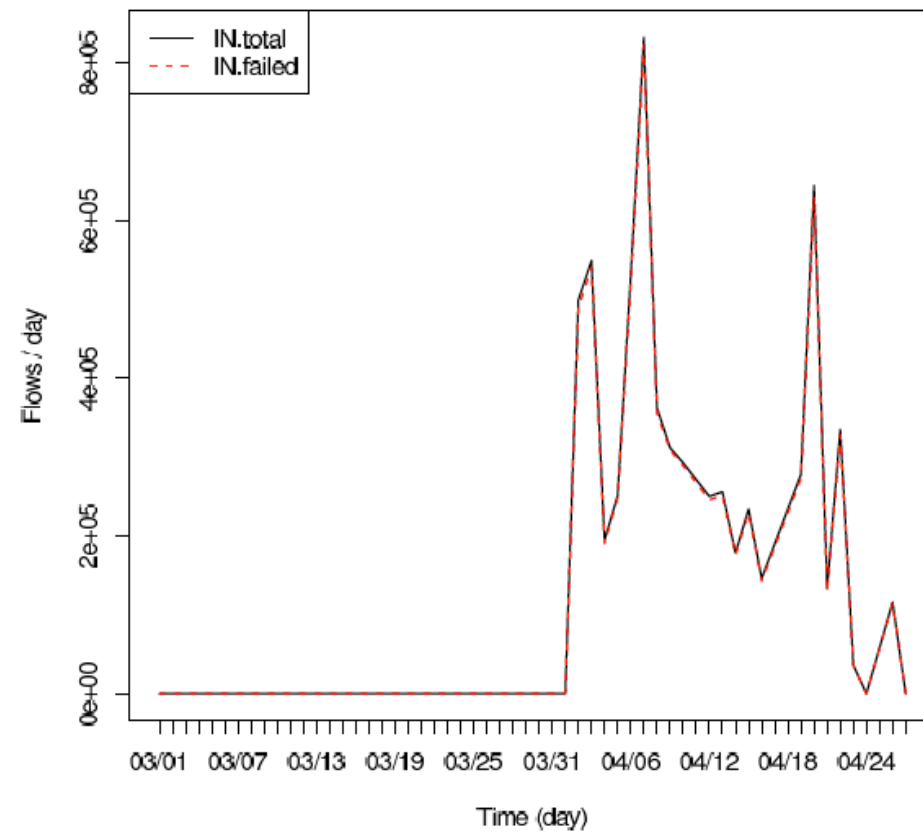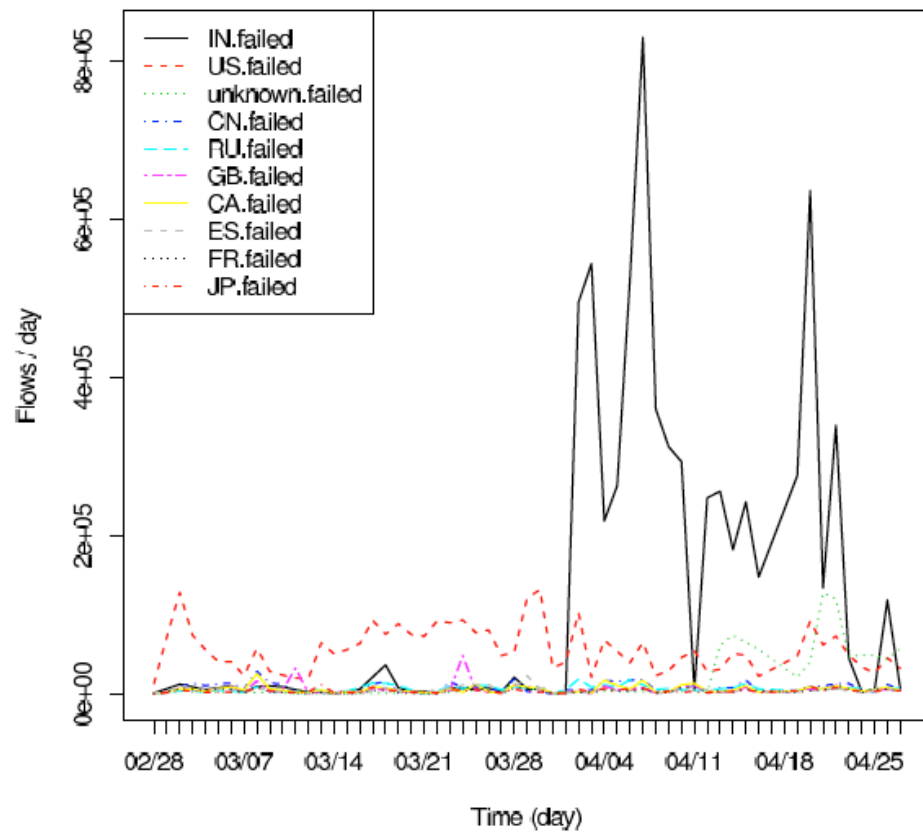
Figure 1: Histogram: Given an IP address, how many blacklisted domains use that IP address as a name server?
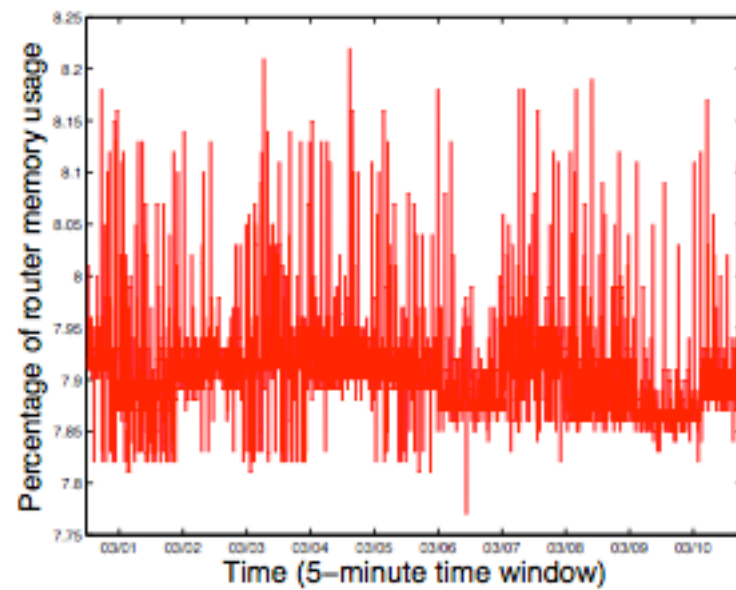
Figure 6: Total memory usage of traffic monitoring system.
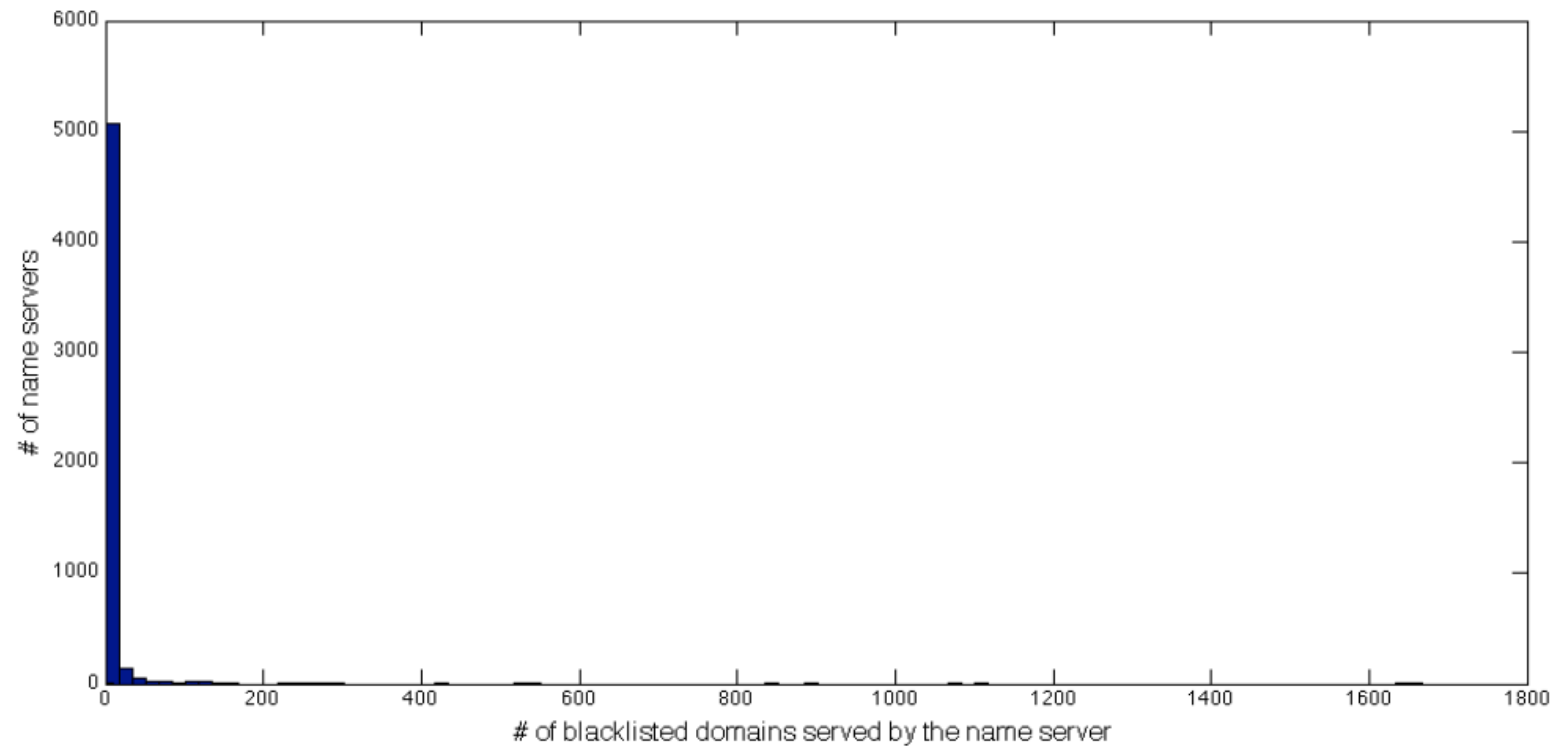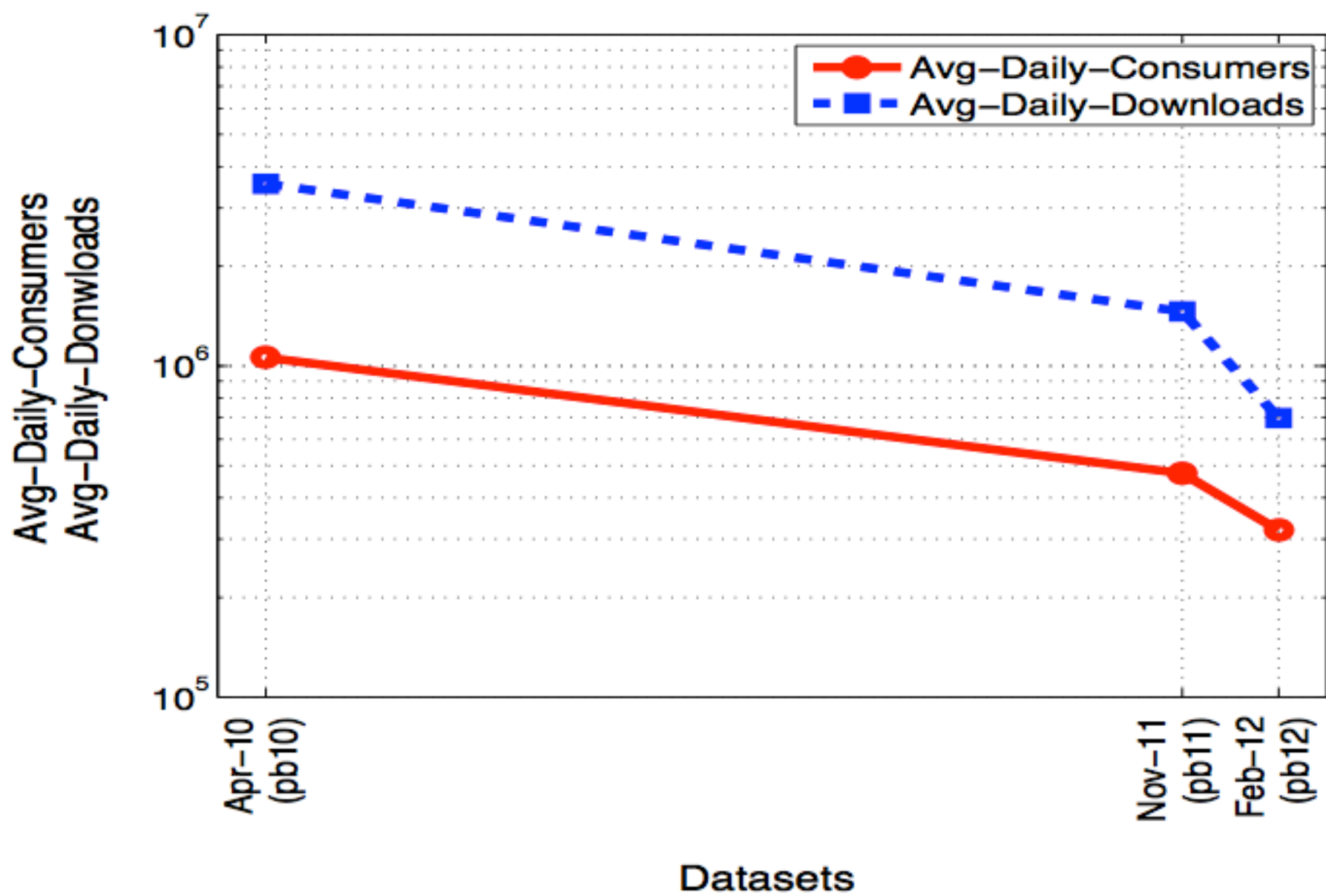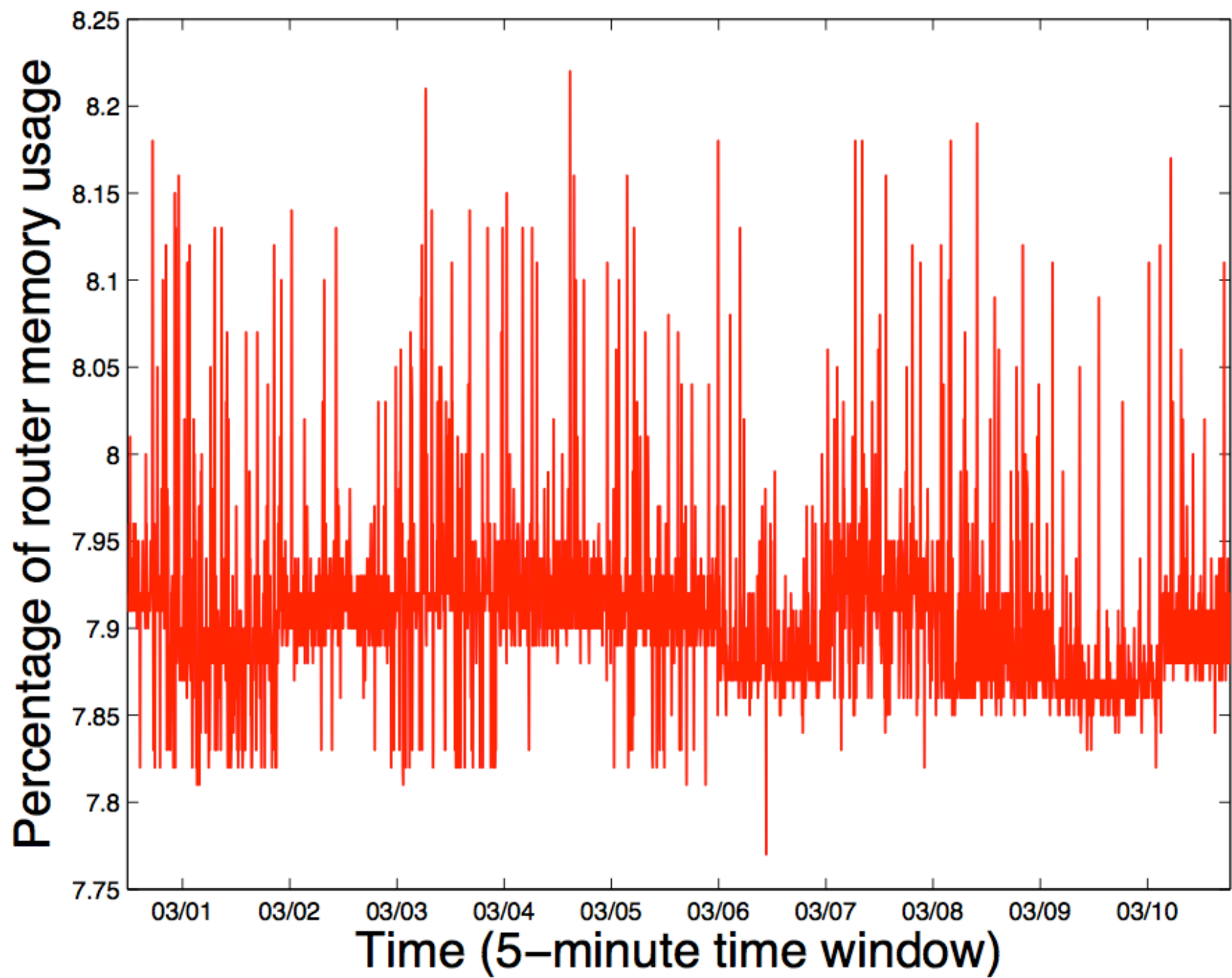
Trace	% Speculatively executed tasks
FB2009	1.22
FB2010	2.04
CC_b	1.01
CC_e	1.4

Trace	% of tasks that straggled even when they executed locally
FB2009	26.4
FB2010	39.2
CC_b	55
CC_e	56

Trace	% of speculatively executed tasks that were killed
FB2009	77.9
FB2010	88.6
CC_b	74.4
CC_e	48.8

Trace	% of tasks speculatively executed, locally that were killed
FB2009	57.57
FB2010	87.12
CC_b	97.4
CC_e	83.96

boottime
365
1395451911 1395451911 1395451911

bytes_in
192 72 49 10 23 4 2 10 0 1 0 0 2
946.52 9406525.26 18812104

bytes_out
235 27 48 28 3 10 1 8 1 1 0 0 2 1
4922.48 16756419.24 33507916

cpu_aidle
365
0 0 0

cpu_idle
48 18 32 63 44 72 88
0.4 49.85 99.3

cpu_nice
365
0 0 0

cpu_num
365
4 4 4

cpu_speed
365
1800 1800 1800

cpu_system
79 80 53 56 35 36 15 7 0 4
0.1 7.55 14.99

cpu_user
96 83 37 68 23 21 37
0.1 44.95 89.8

cpu_wio
76 18 4 10 6 4 7 1 0 0 2 0 0 0 0 1
0.1 23.65 47.2

dfs.datanode.blockChecksumOp_avg_time
365
0 0 0

dfs.datanode.blockChecksumOp_num_ops
365
0 0 0

dfs.datanode.blockReports_avg_time
5 3 1 0 1 0 0 0 1 1 1 2 350
14 26.5 39

dfs.datanode.blockReports_num_ops
0 0.01 0.01

dfs.datanode.blocks_get_local_pathinfo
365
0 0 0

dfs.datanode.blocks_read
223 37 30 20 16 7 24 8
0 1.58 3.16

dfs.datanode.blocks_removed
206 47 54 14 14 13 10 4 3
0 1.47 2.93

dfs.datanode.blocks_replicated
266 29 23 14 6 4 15 8
0 0.07 0.14

dfs.datanode.blocks_verified
9 3 4 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 1
0 0.13 0.27

dfs.datanode.blocks_written
222 95 13 12 0 0 3 12 6 0 0 0 2
0 3.11 6.23

dfs.datanode.block_verification_failures
365
0 0 0

dfs.datanode.bytes_read
254 27 20 13 14 23 0 14
0 23334290.78 46668581.56

dfs.datanode.bytes_written
287 22 24 10 8 1 2 3 1 2 2 1
0 17408923.6 34817847.19

dfs.datanode.copyBlockOp_avg_time
365
0 0 0

dfs.datanode.copyBlockOp_num_ops
365
0 0 0

dfs.datanode.heartBeats_avg_time
32 6 21 48 26 15 0 1 0 0 0 0 0 0 0 0 0 0 2
0.67 2.33 4

dfs.datanode.heartBeats_num_ops
240 36 35 14 8 14 14 1 0 3
0 1.33 2.67

dfs.datanode.readBlockOp_avg_time
209 30 34 42 22 14 0 4 10

dfs.datanode.readBlockOp_num_ops
258 31 18 16 25 3 1 6 4 3

dfs.datanode.reads_from_local_client
259 26 24 15 2 16 15 4 0 3 0 1

dfs.datanode.reads_from_remote_client
234 36 30 21 10 16 8 8 0 1 1

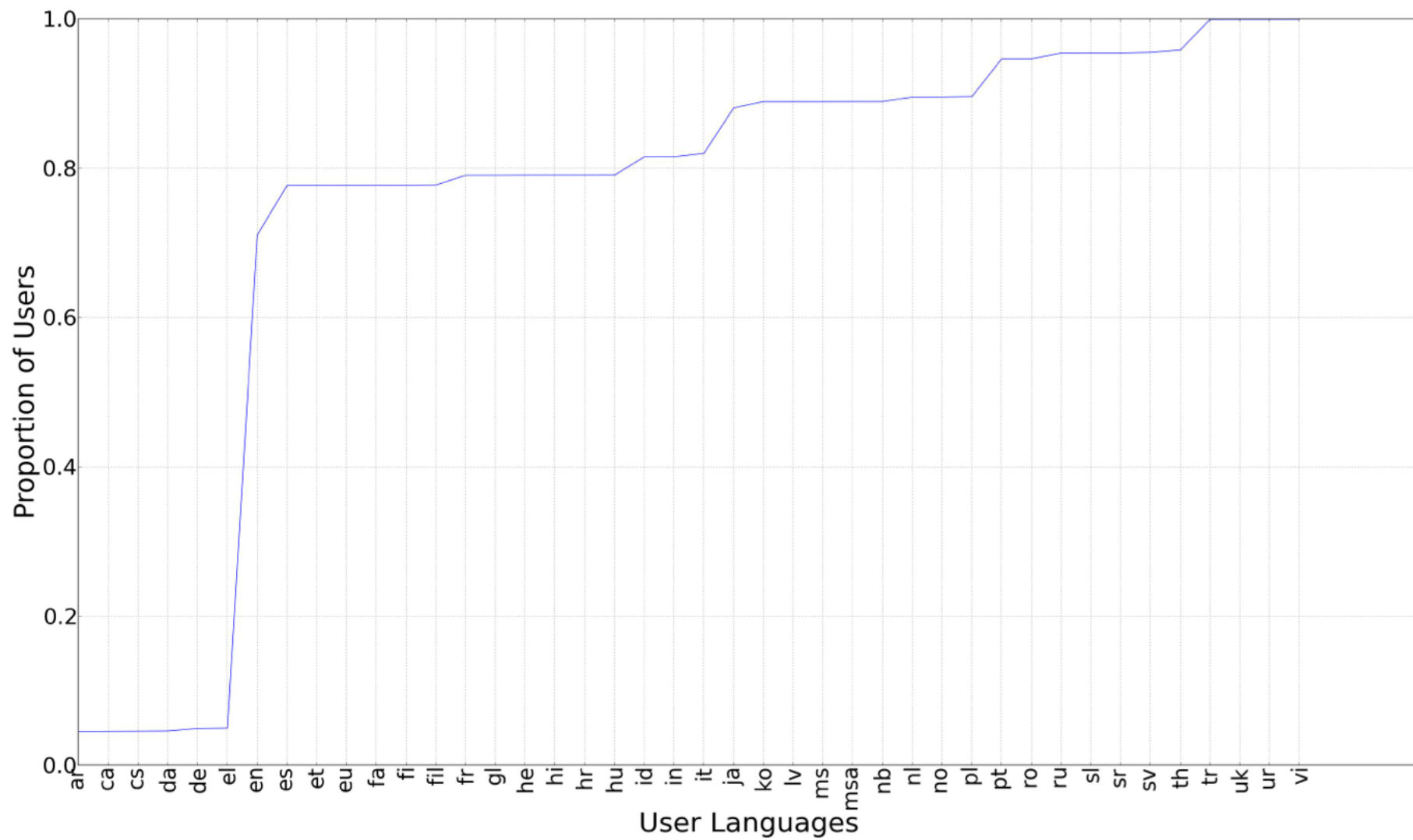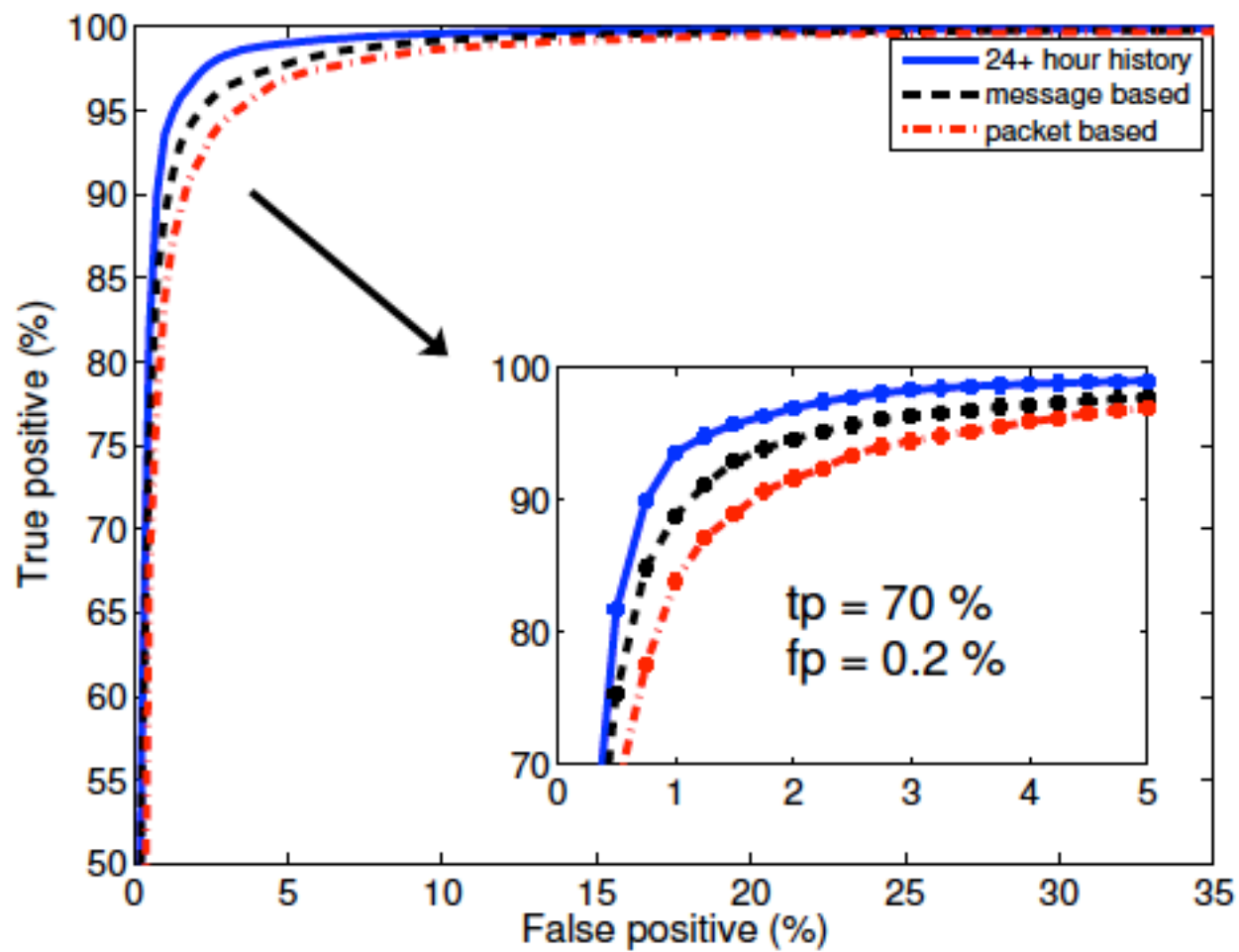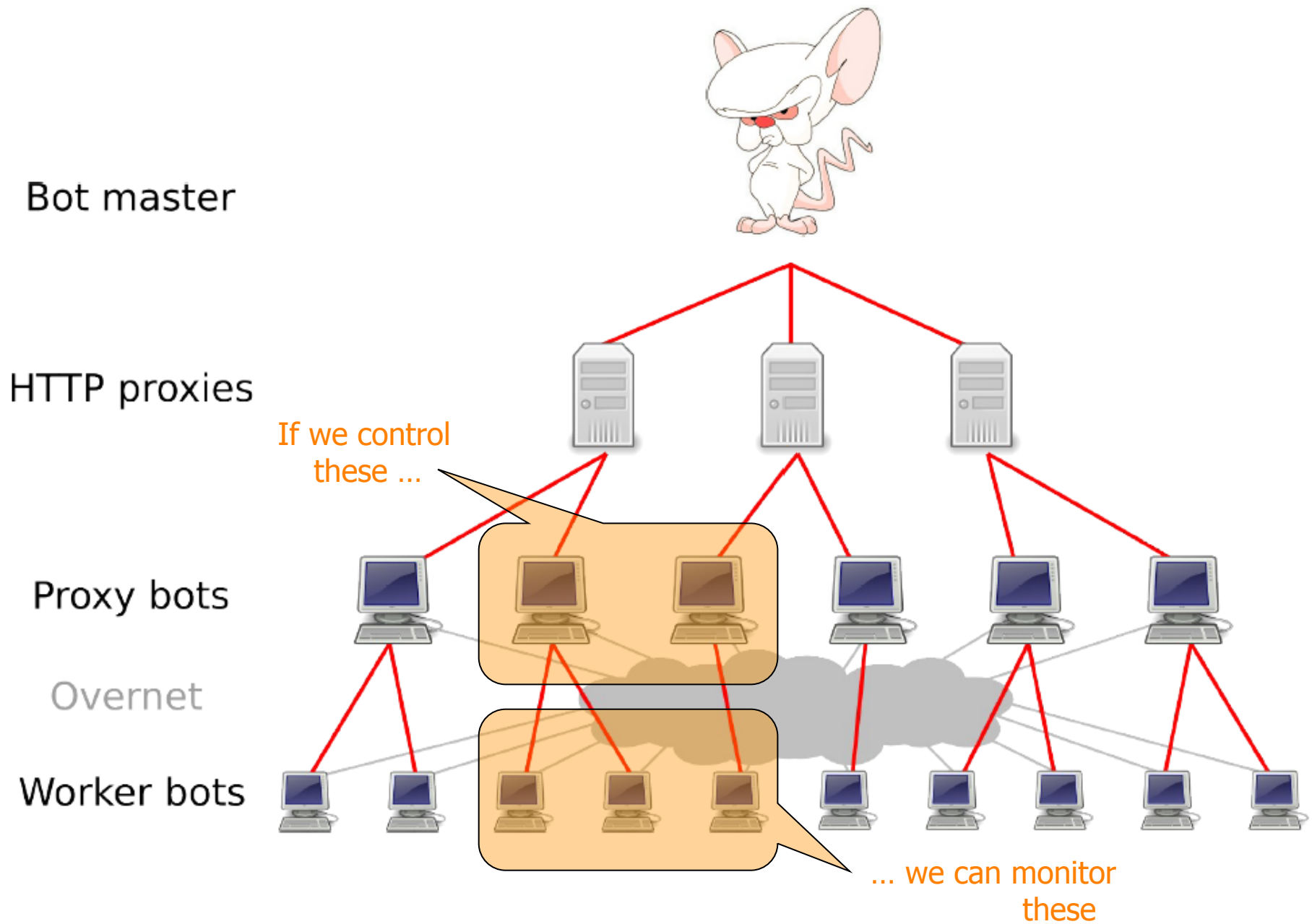(a) Number of Followers for Cluster Users and a Random Sample of Users

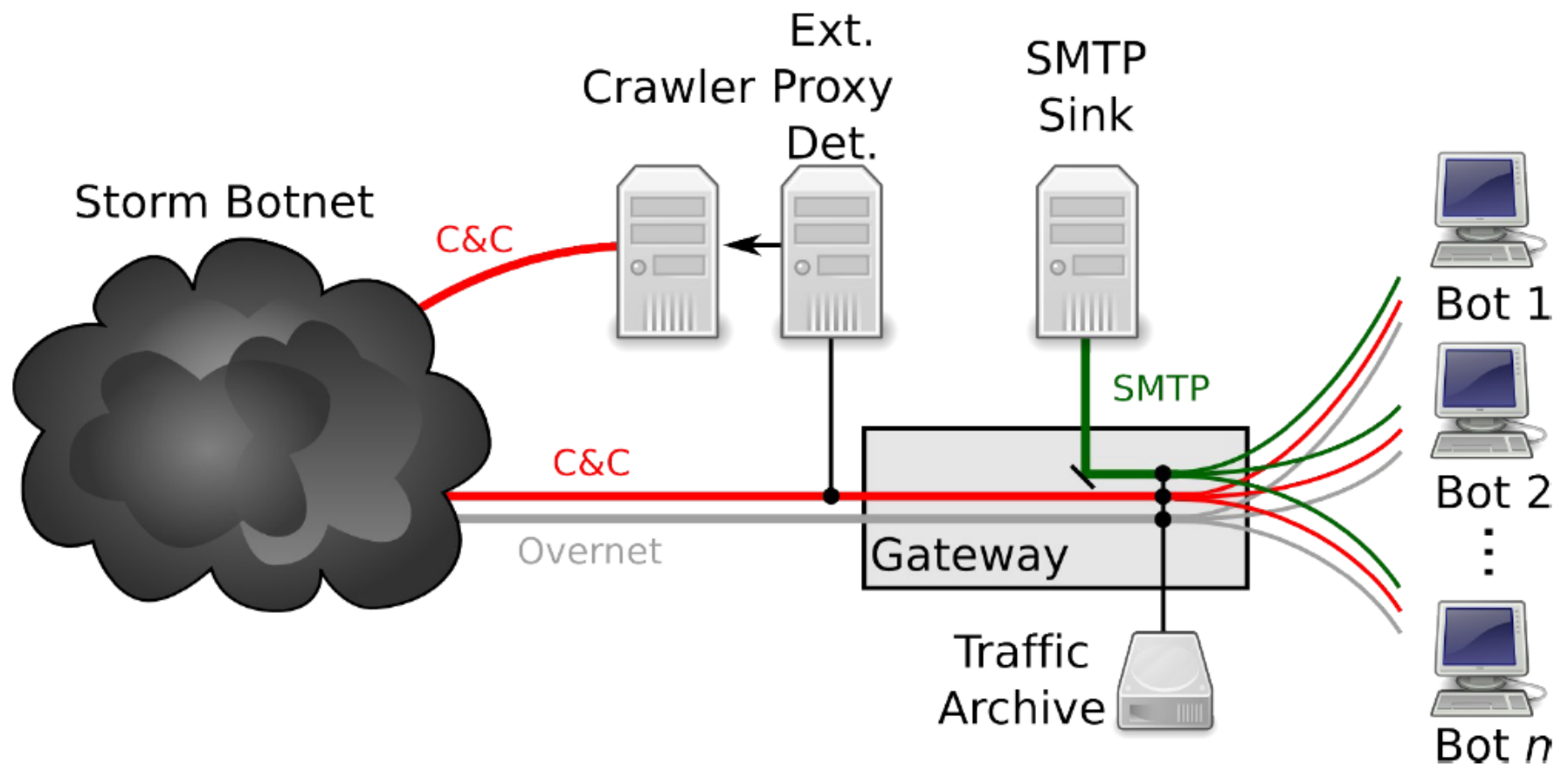Fig. 7: CDF of user account languages for users in size 2 clusters

ROC in SNARE

Storm Botnet

Ext.
Crawler Proxy
Det.

SMTP
Sink

C&C

C&C

Overnet

Gateway

SMTP

Traffic
Archive

Bot 1

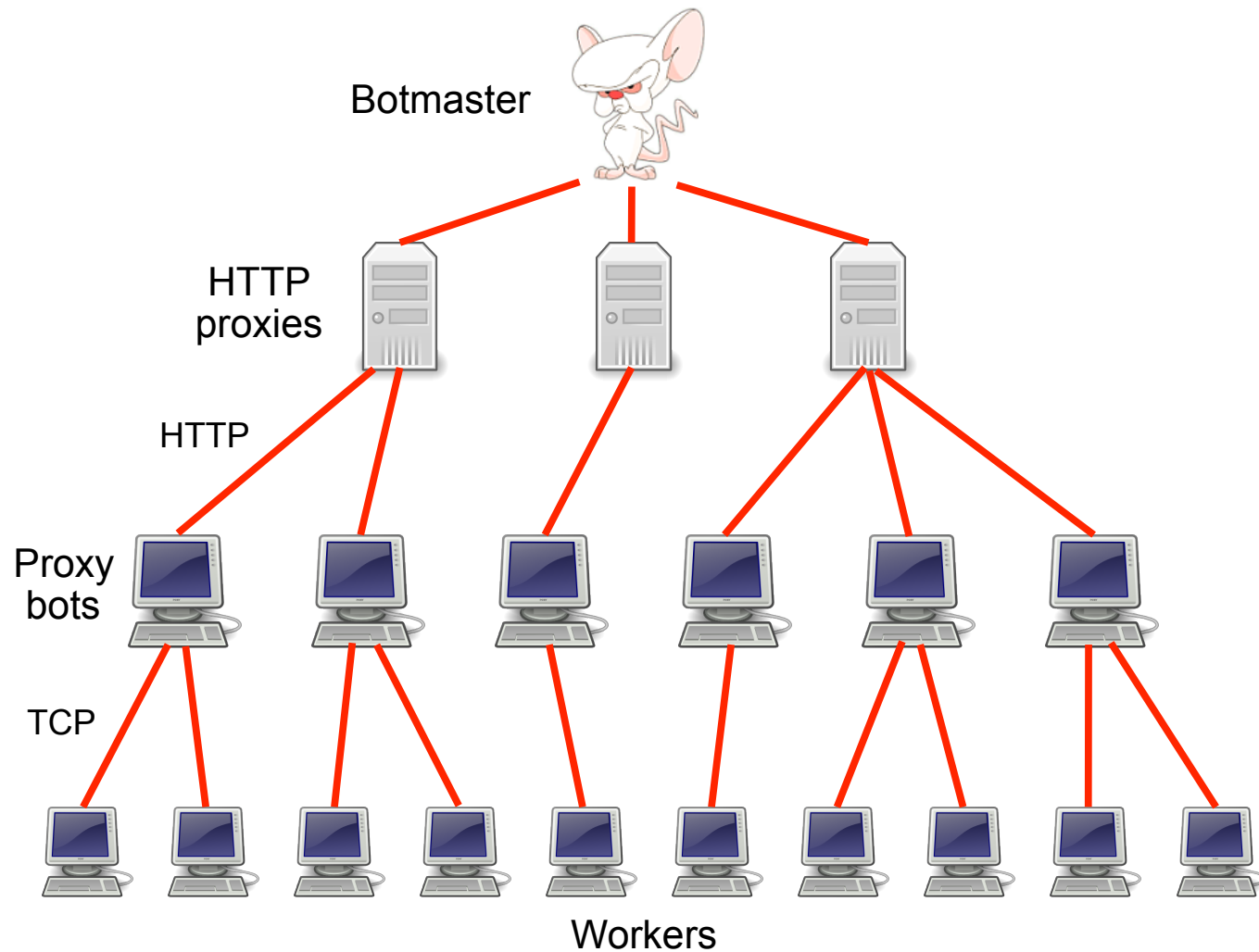Bot 2

Bot *n*

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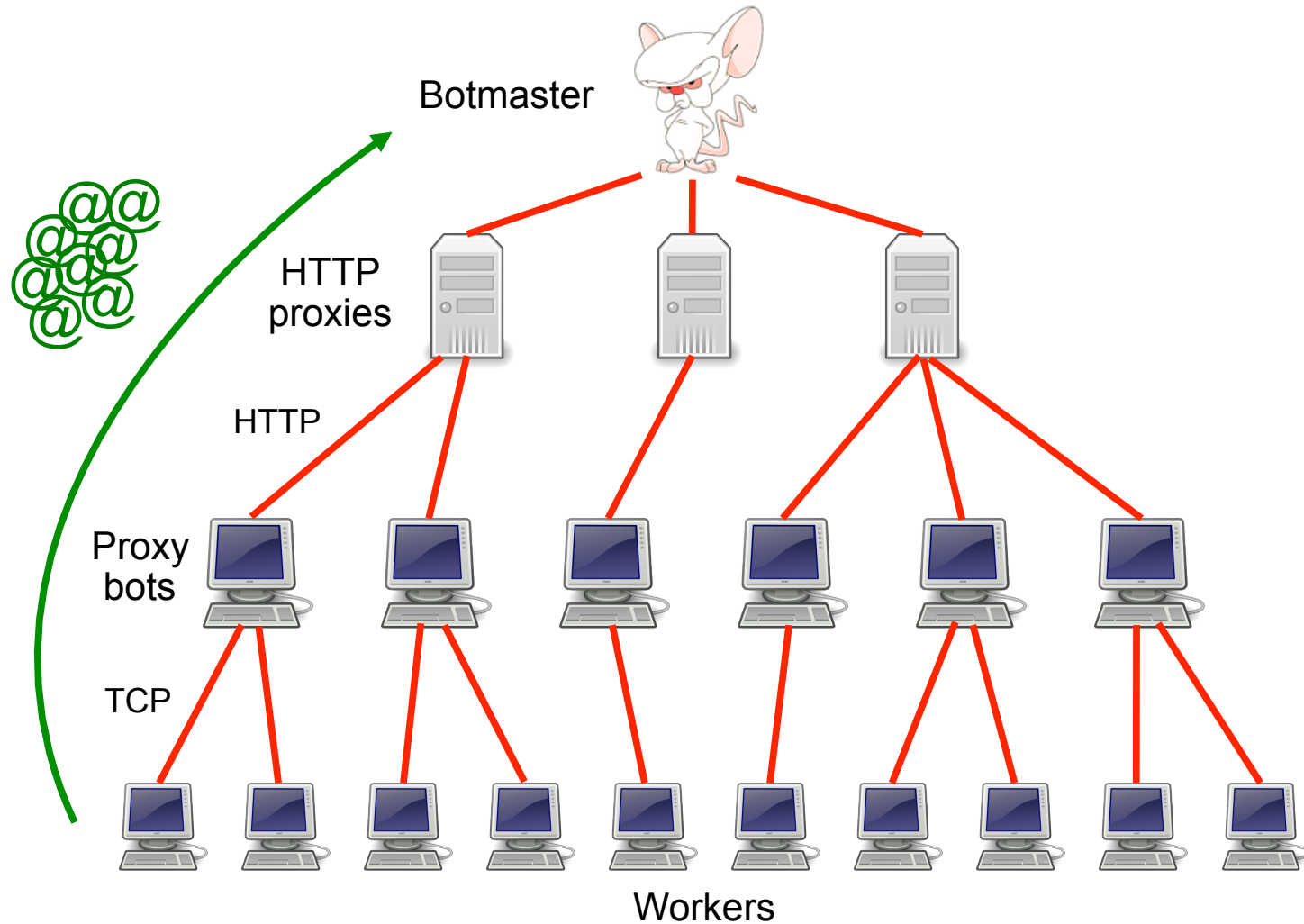
- Activation (report from bot to botmaster)
- Email address harvests
- Spamming instructions
- Delivery reports
- DDoS instructions
- FastFlux instructions
- HTTP proxy instructions
- Sniffed passwords report
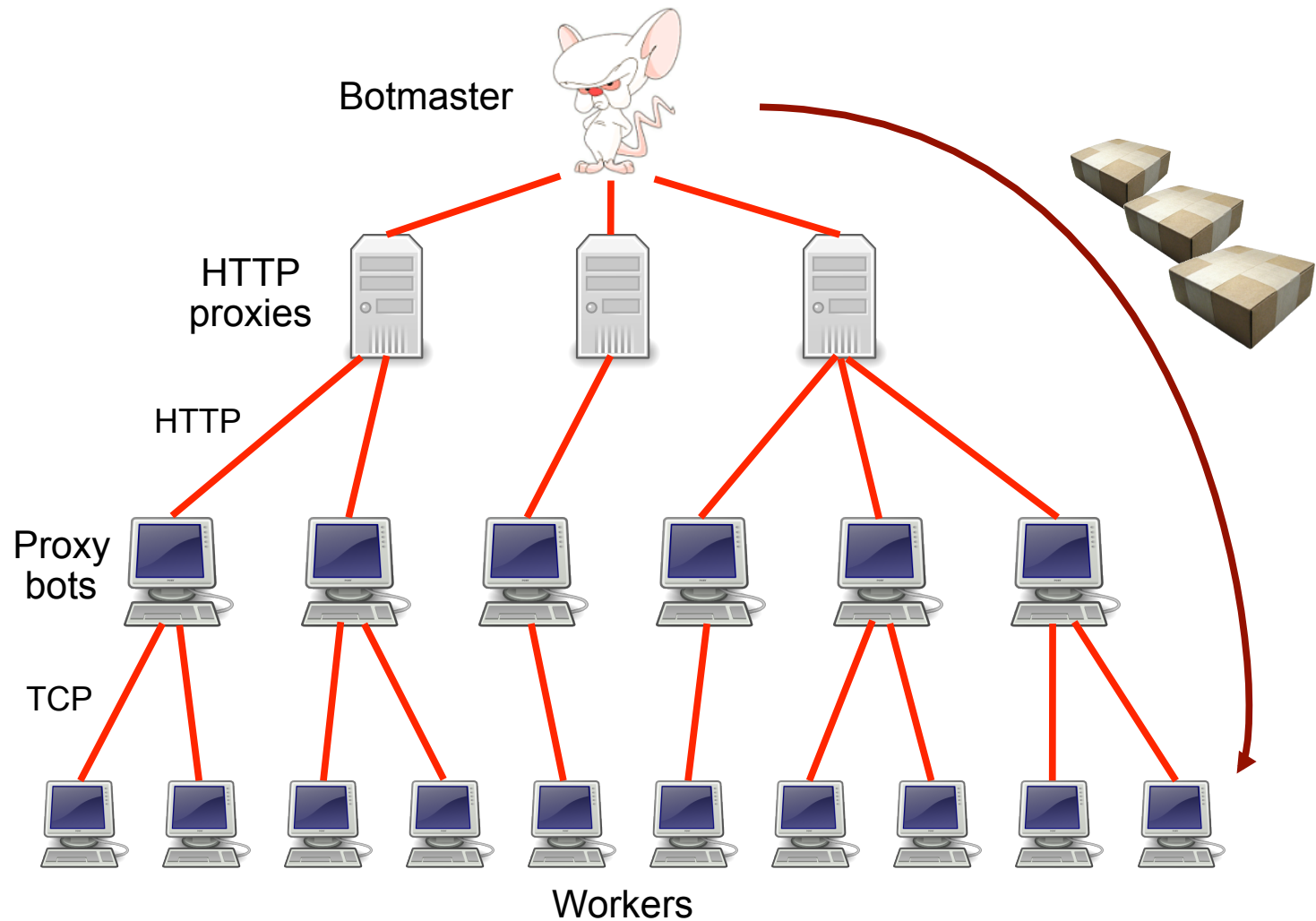- IFRAME injection/report

Spam campaign mechanics

Botmaster

HTTP proxies
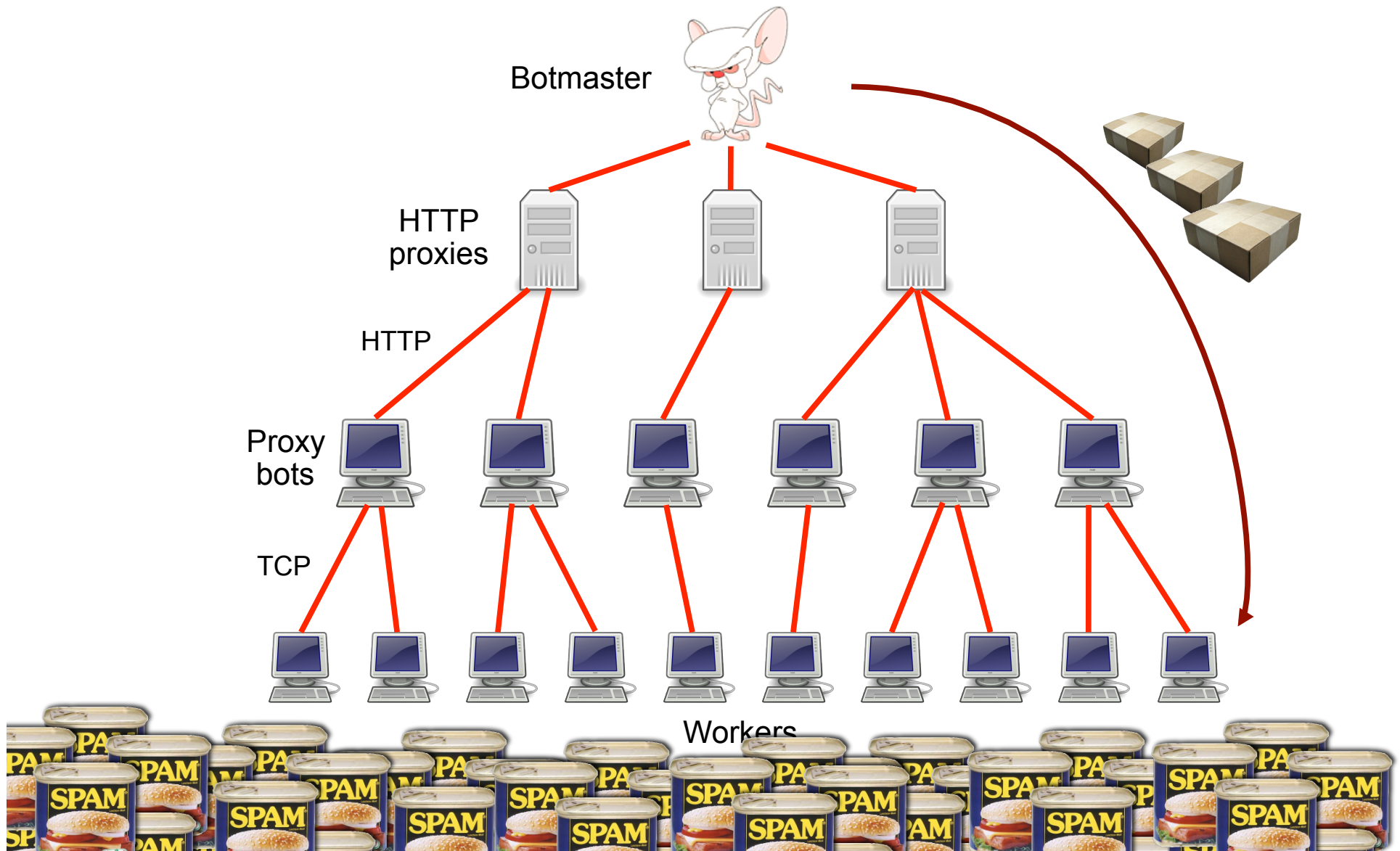
HTTP

Proxy bots

TCP

Workers

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

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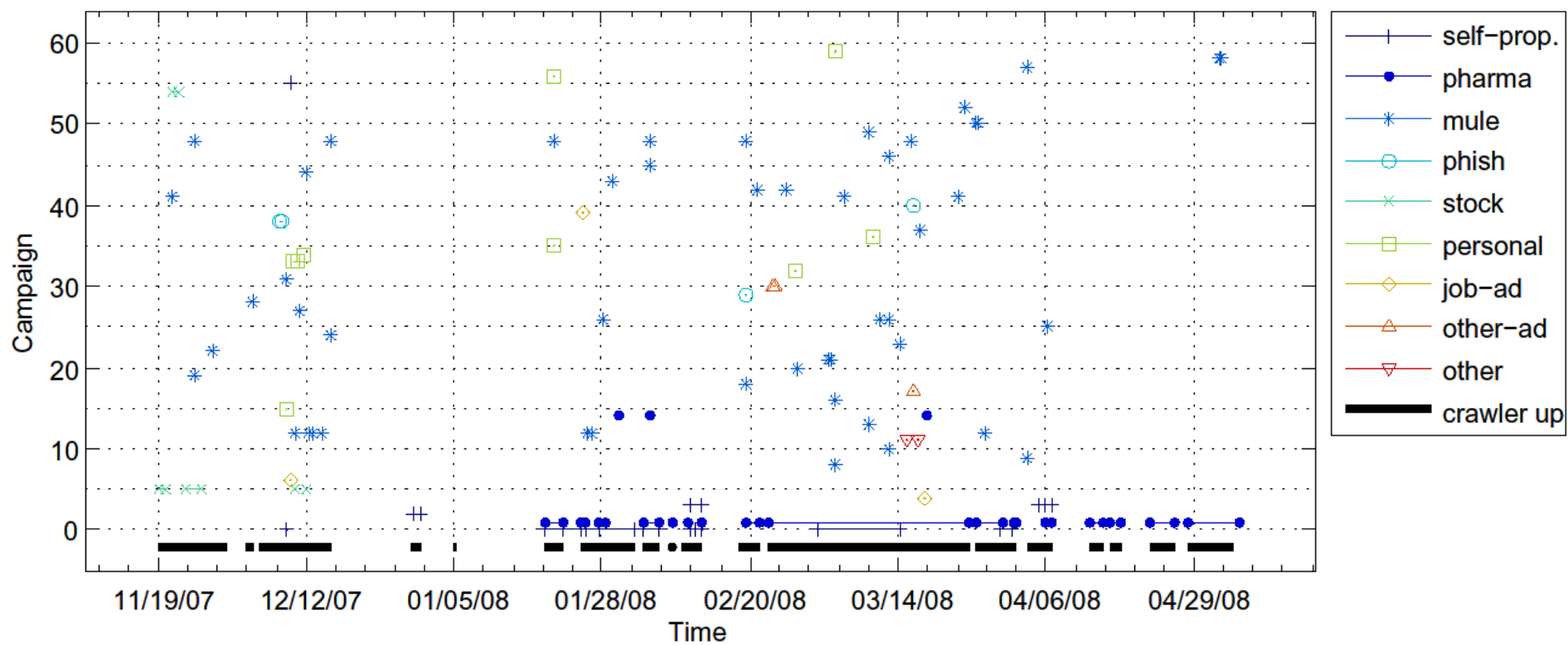
Figure 5: Classes and instances of spaming campaigns identified over time.

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
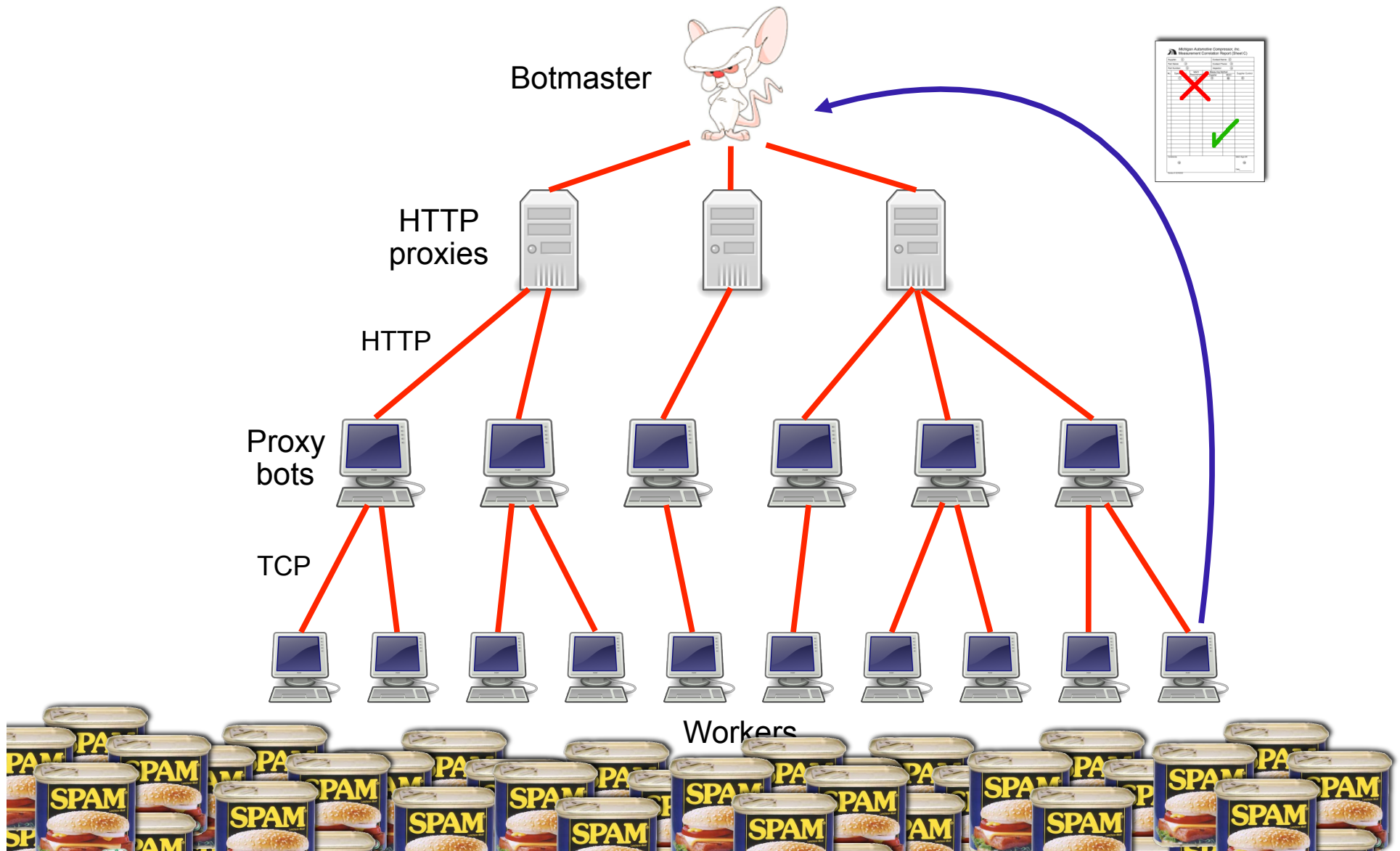
Measurements: delivery efficacy