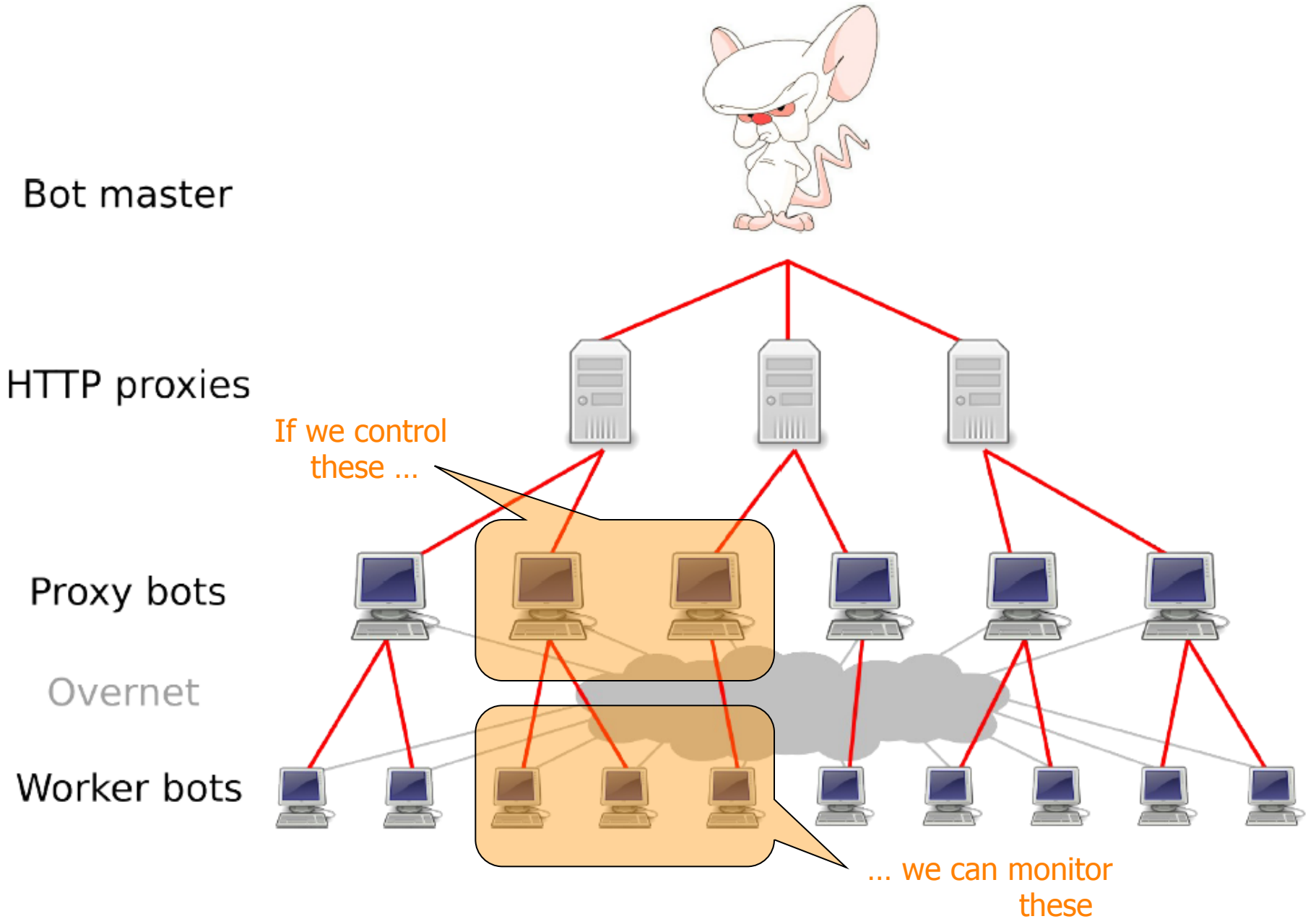
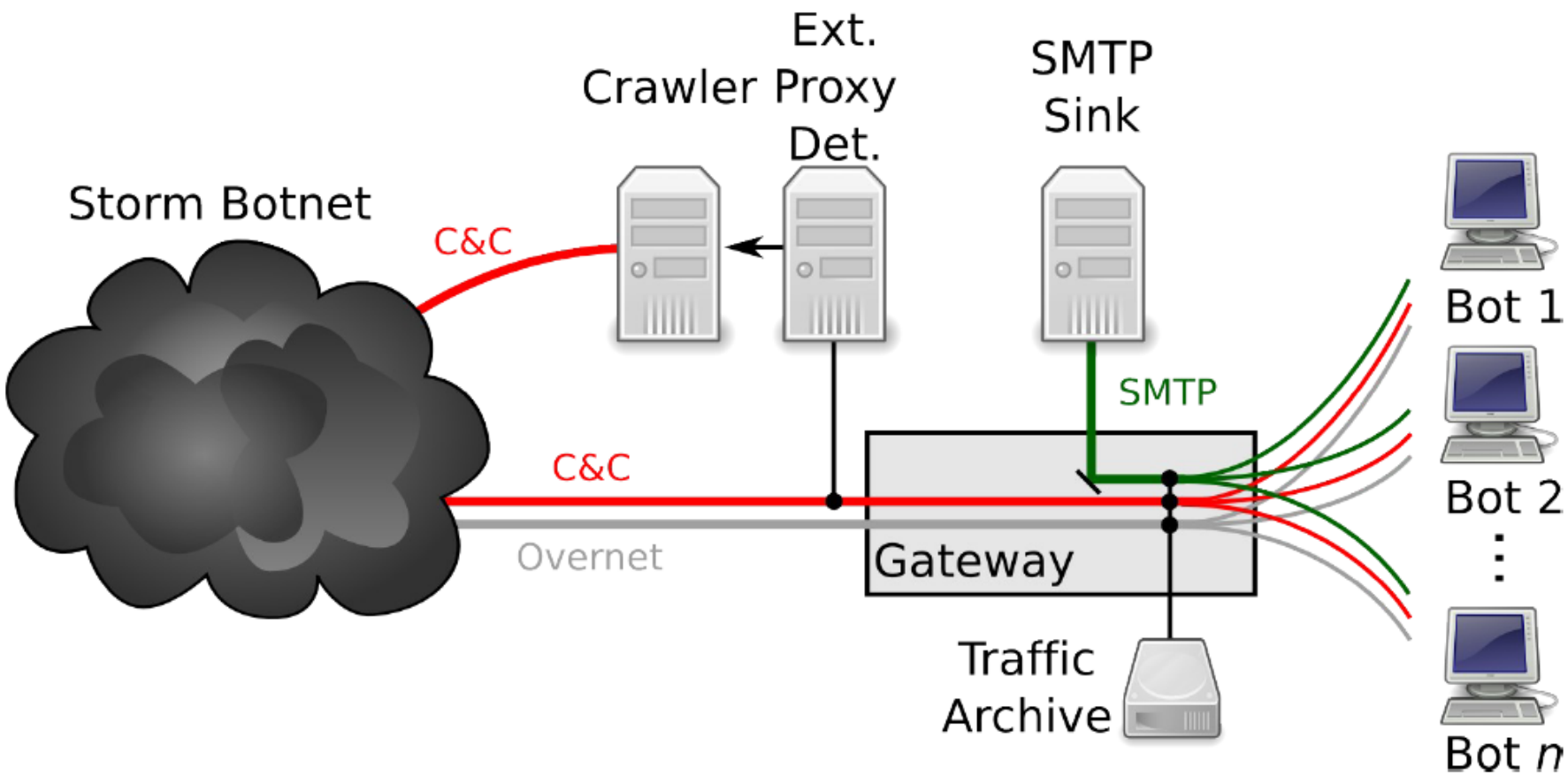
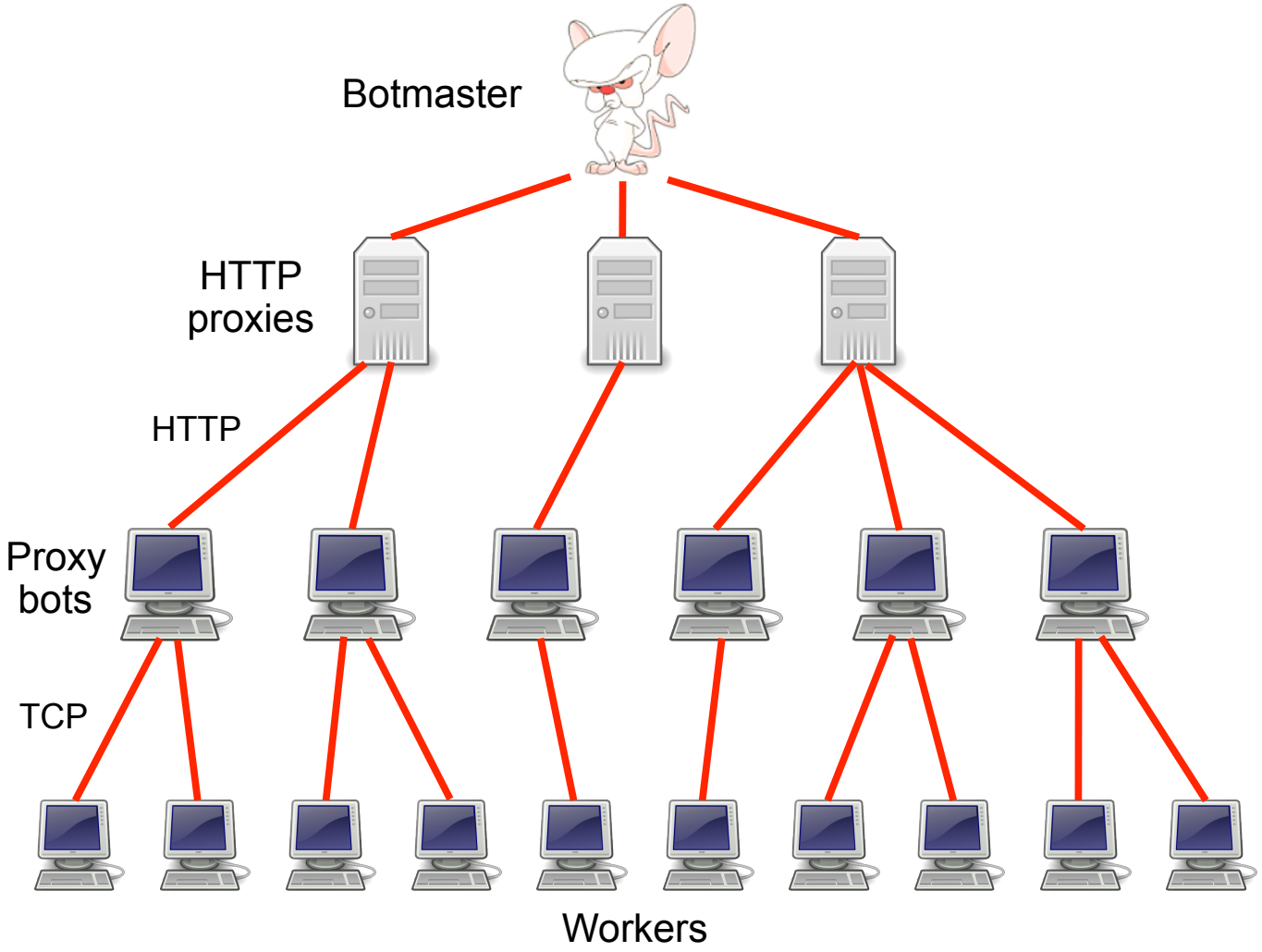

Bot master
HTTP proxies
If we control these …
Proxy bots
Overnet
Worker bots
… we can monitor these


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

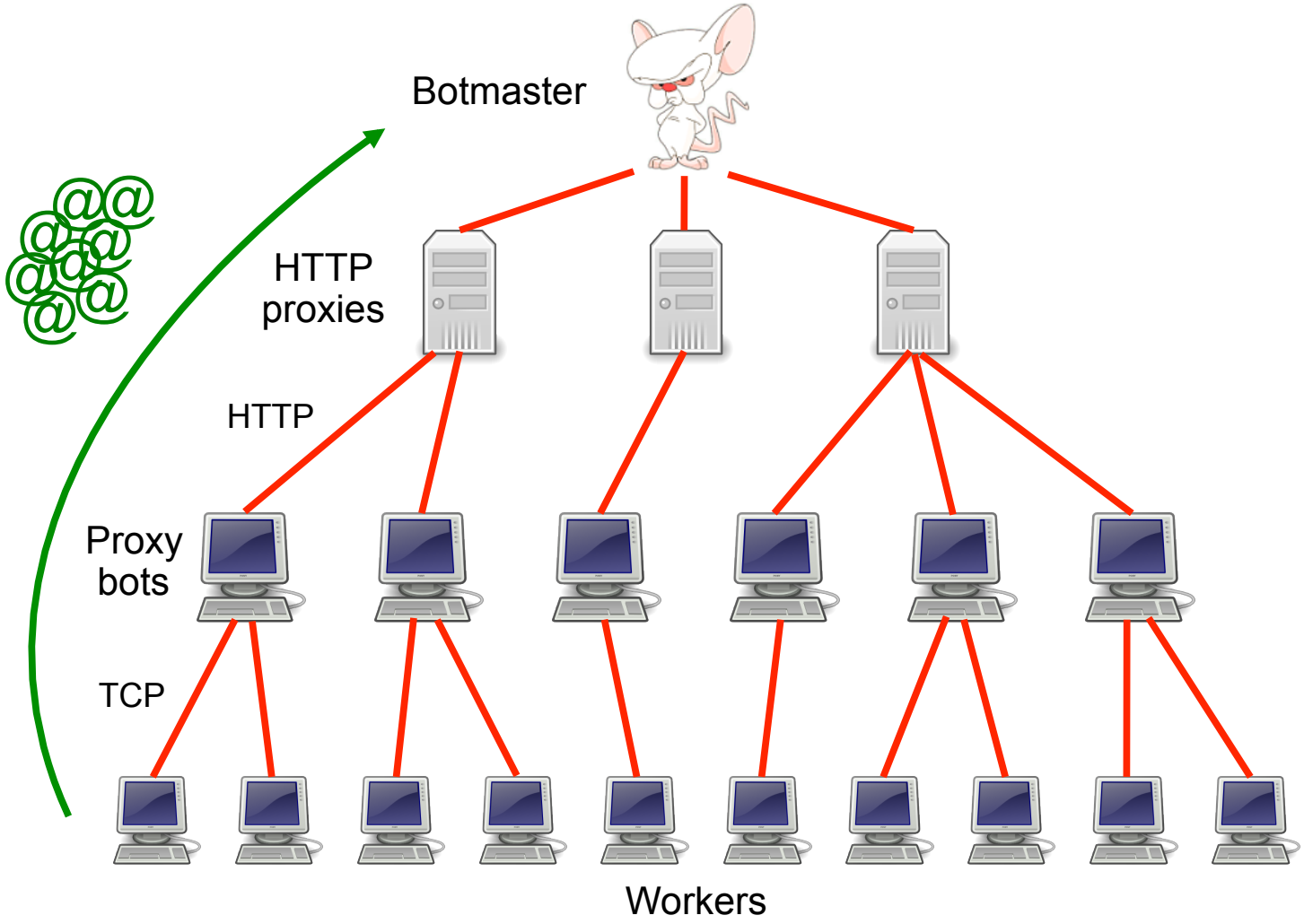
Types of Storm C&C Messages

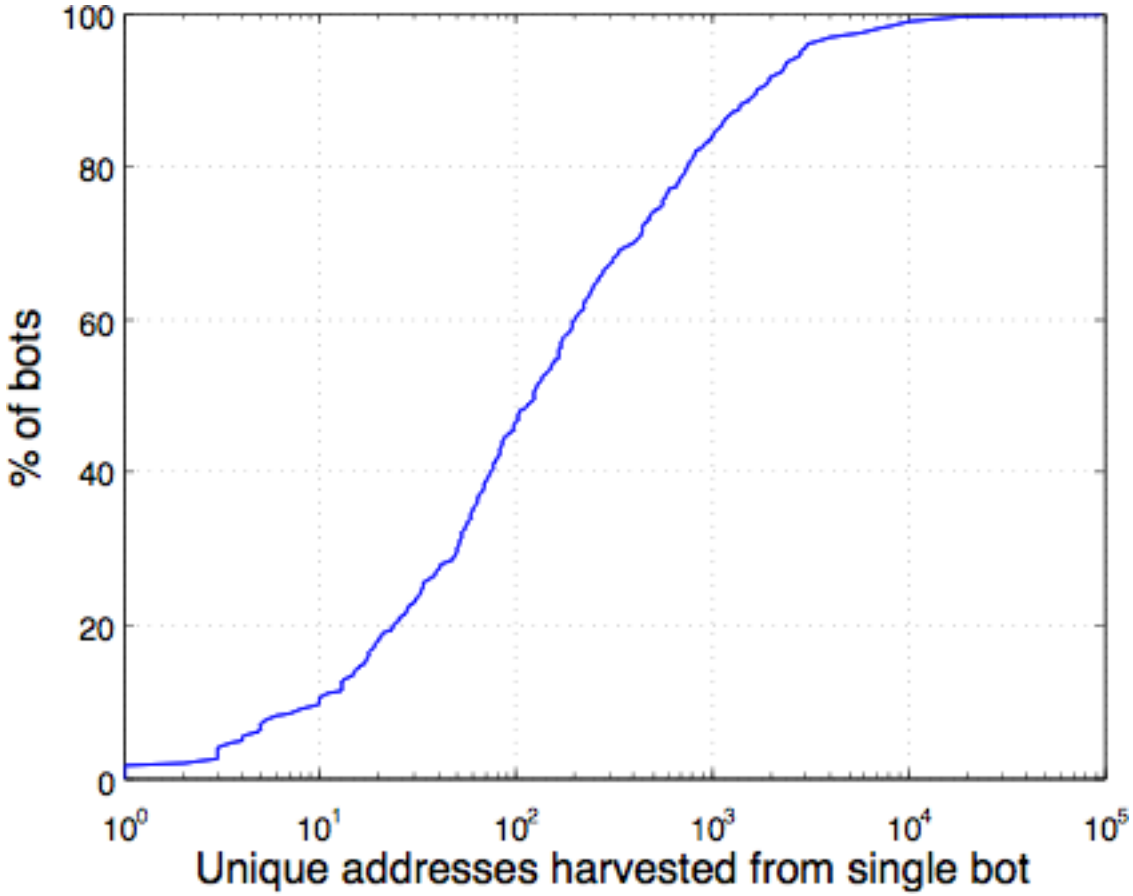
- Activation (report from bot to botmaster)
- Email address harvests
- Spamming instructions
- Delivery reports
- DDoS instructions
- FastFlux instructions
- HTTP proxy instructions
- Sniffed passwords report
- IFRAME injection/report

Spam campaign mechanics

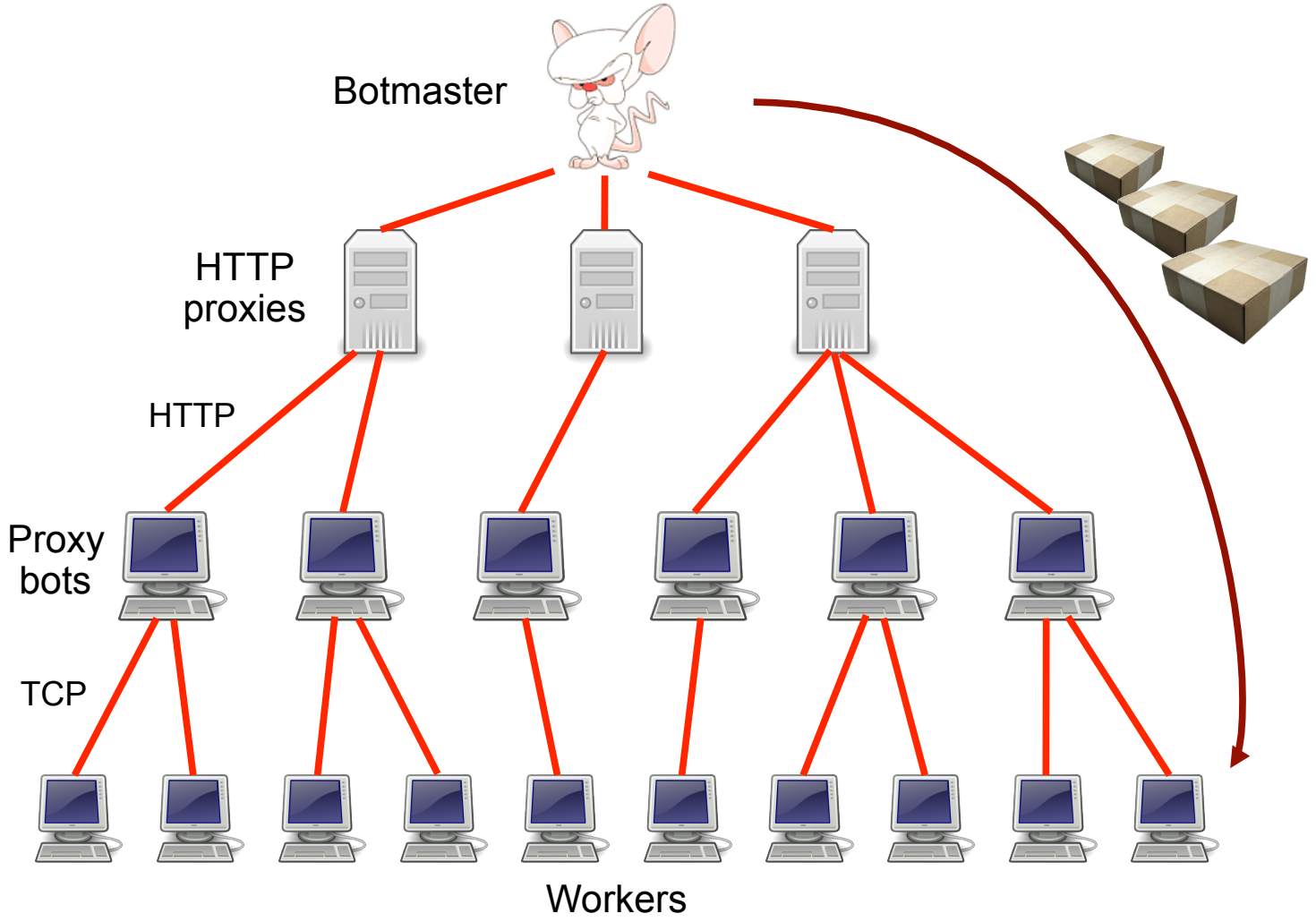


Campaign mechanics: harvest




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.

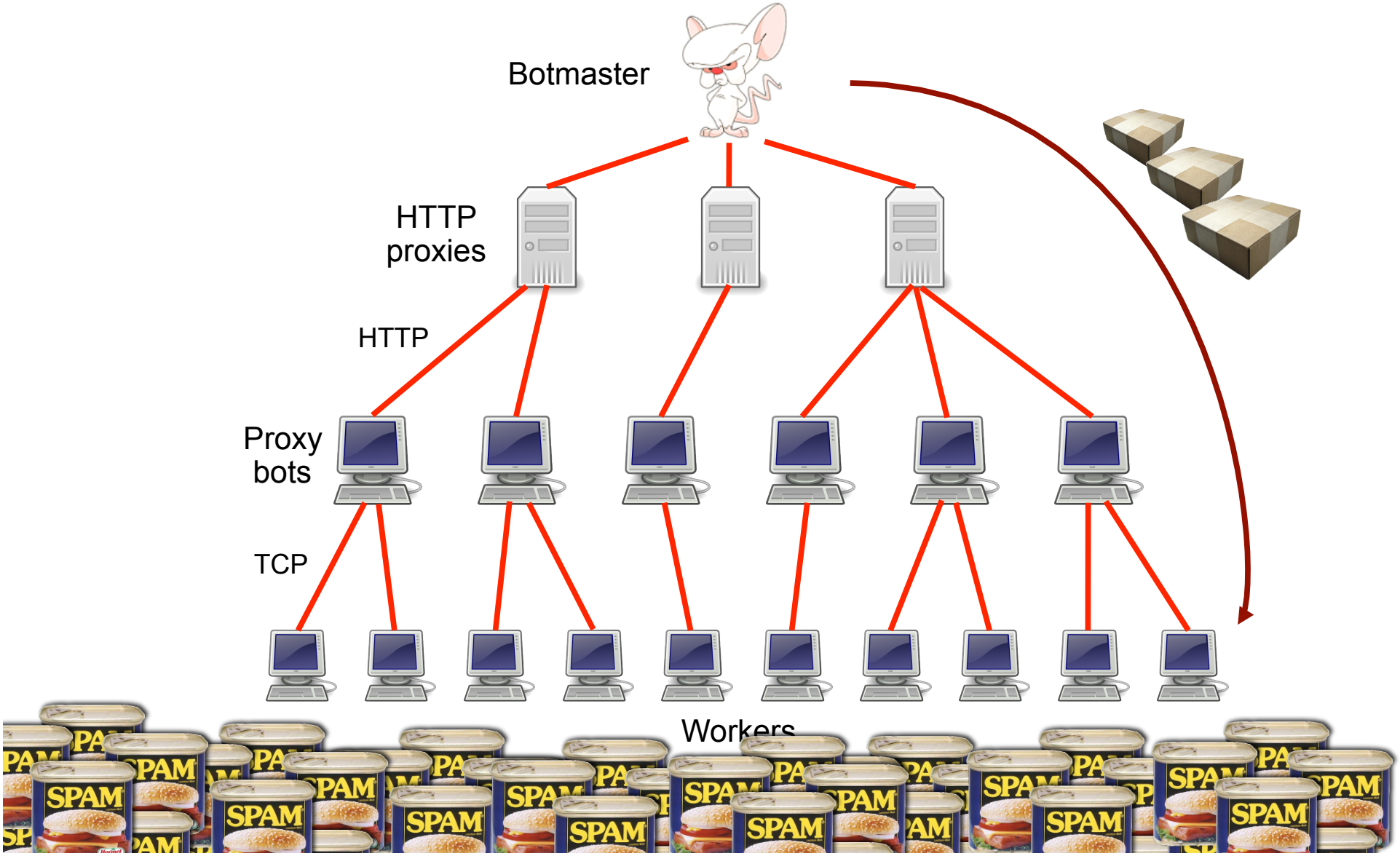
Table 2: Storm's spam-generation templating language.

```
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.

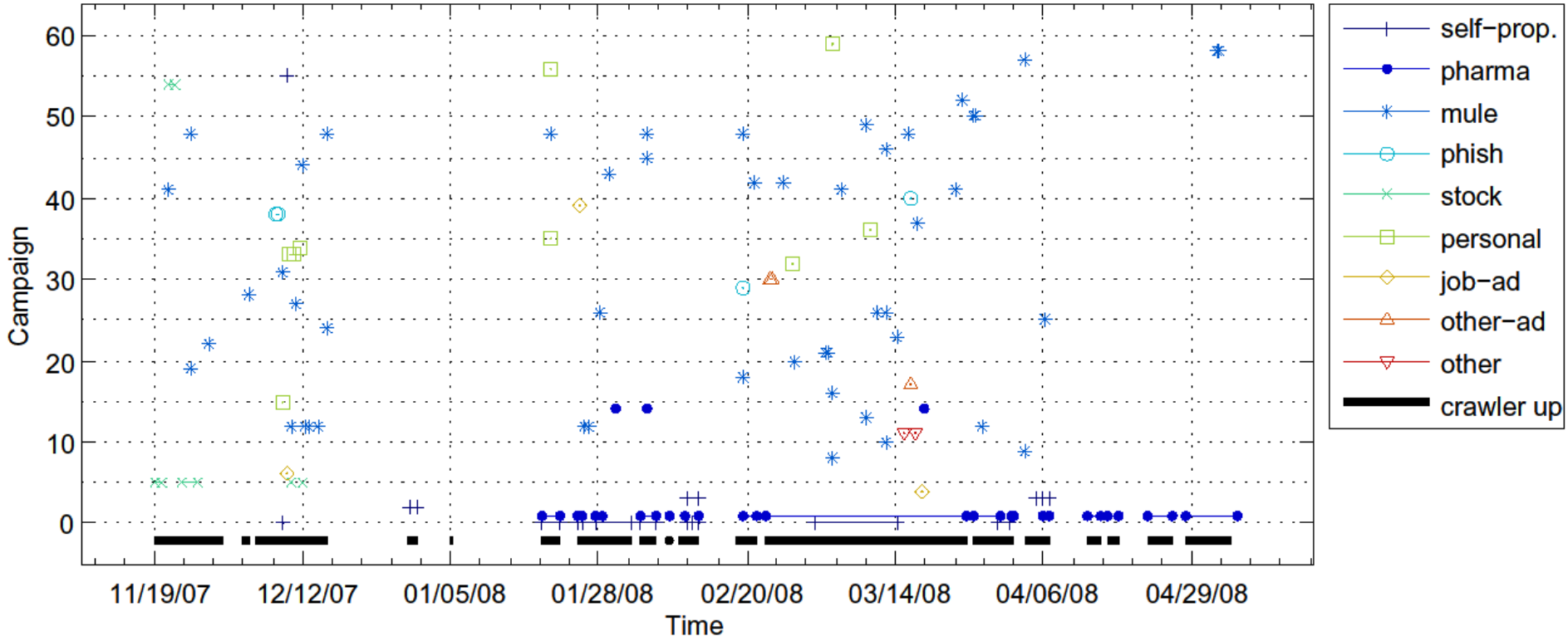
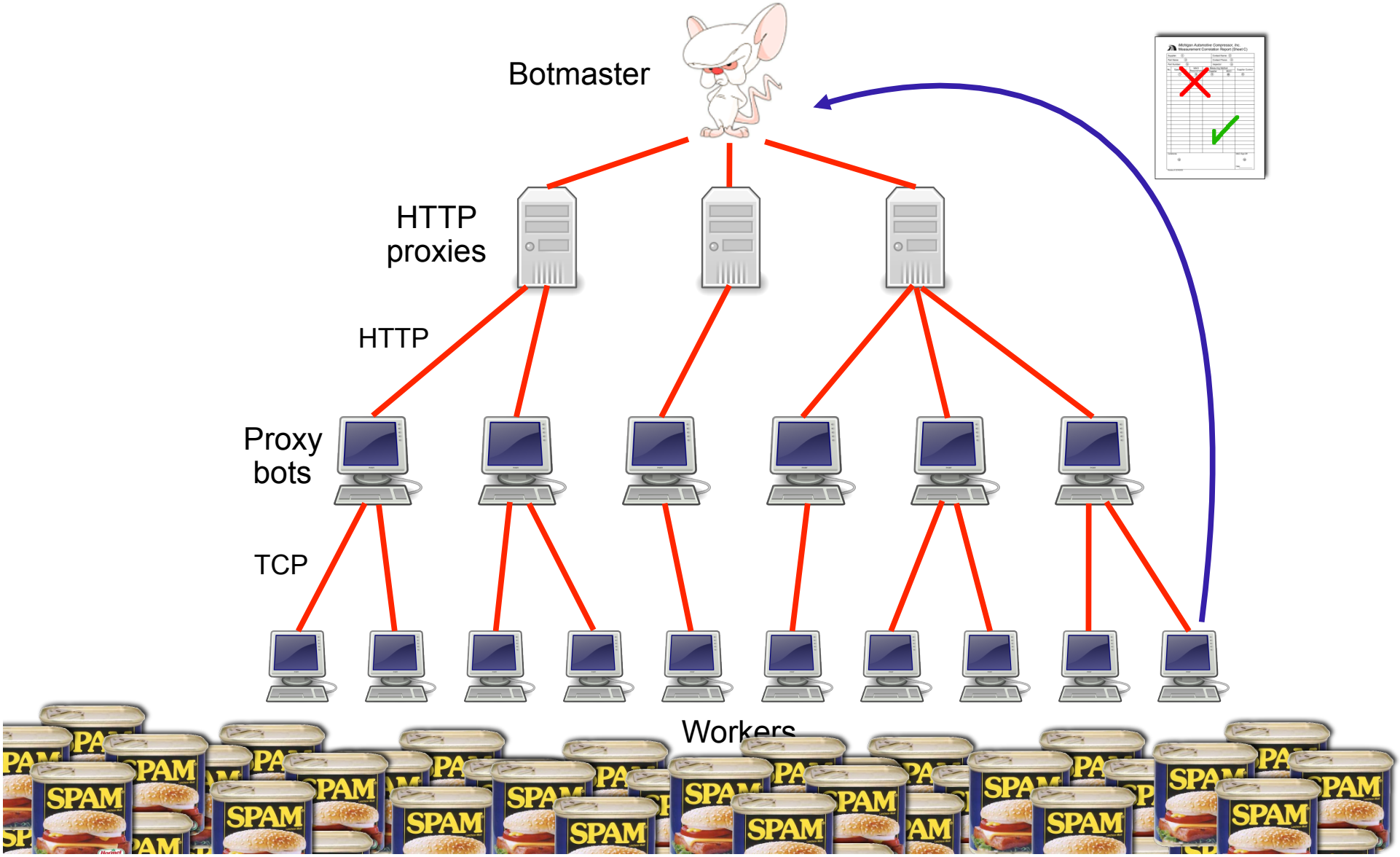


Figure 5: Classes and instances of spaming campaigns identified over time.

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