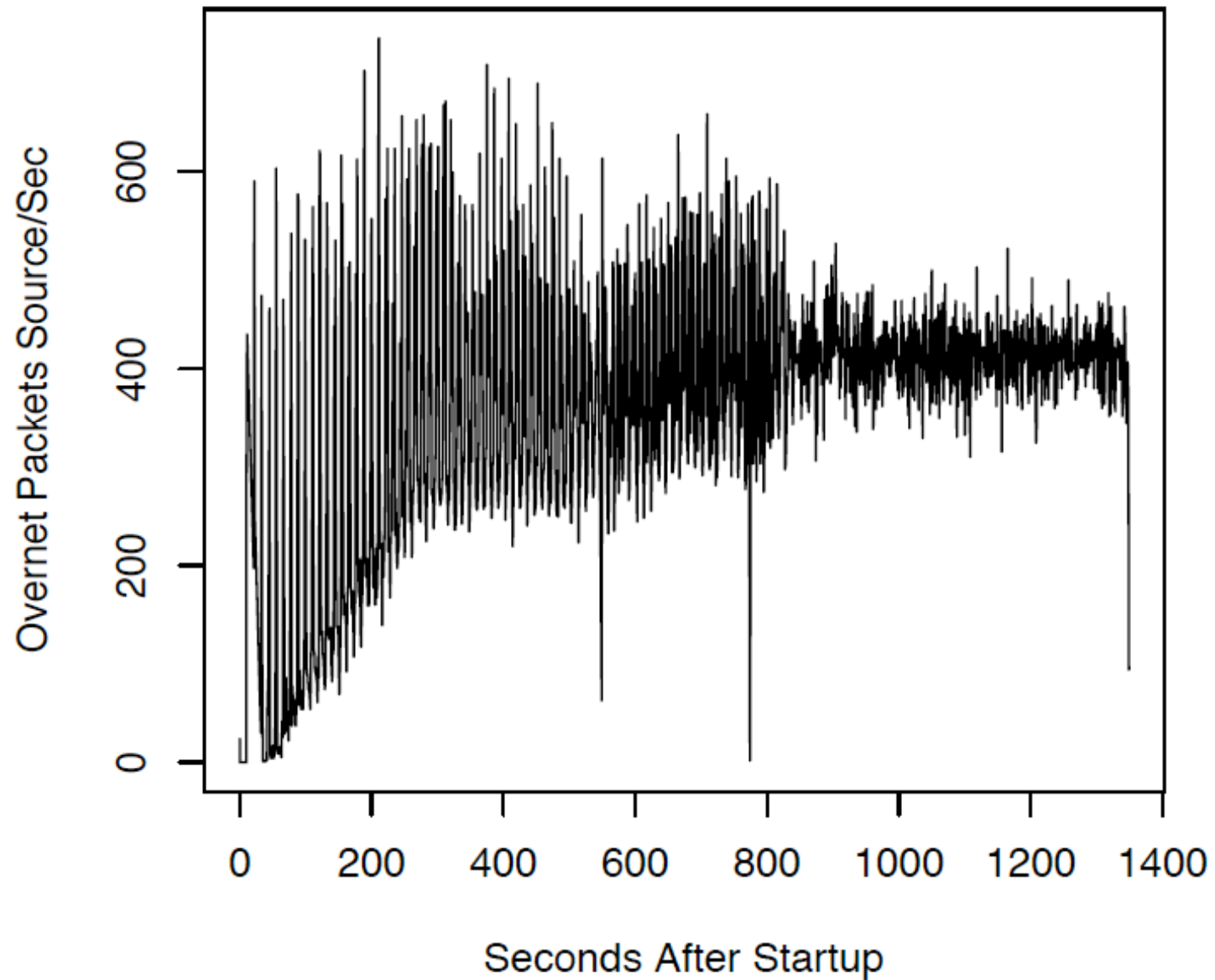


Figure 2: Architecture overview of our BotMiner detection framework.

Storm Worker Bot Activity – 10,652 Destinations

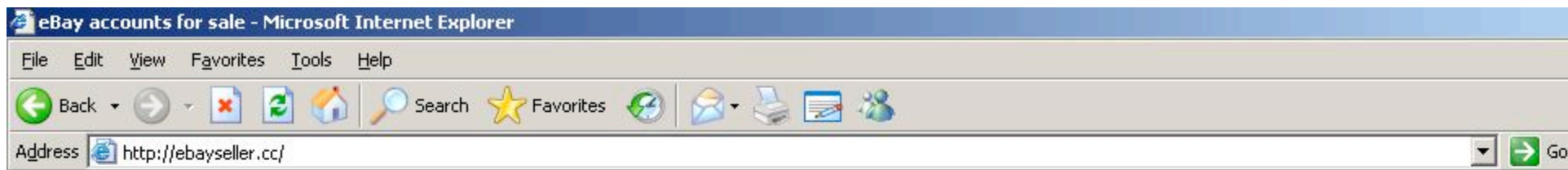


Сейчас в наличии

| Служба | Кол-во акков | Цена за 1K акков |
|------------------------|--------------|---|
| Mail.ru | 3046 | до 10K: \$10 от 10K до 100K: \$8 от 100K: \$6 |
| Pochta.ru (+ FTP) | 35 | до 10K: \$8 от 10K до 100K: \$5 от 100K: \$4 |
| Yandex.ru (+ Narod.ru) | 0 | до 10K: \$9 от 10K до 100K: \$7 от 100K: \$5 |
| Gmail.com | 134670 | до 10K: \$6 от 10K до 100K: \$5 от 100K: \$4 |
| Hotmail.com | 42893 | до 10K: \$7 от 10K до 100K: \$6 от 100K: \$5 |
| Yahoo.com | 10847 | до 10K: \$9 от 10K до 100K: \$7 от 100K: \$6 |

Обновить статистику

купить: 100K  Gmail.com 



Список доступных акков

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субъективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.

Перед покупкой следует обязательно ознакомиться с FAQ.

По работе с товаром не консультирую.

Работа через гарант сервис приветствуется.

Мои цены:

seller/баер акк до 10 фидов = 5\$

seller/баер акк 10-25 фидов = 10\$

seller/баер акк 25-50 фидов = 15\$

seller/баер акк более 50 фидов = 25\$



My Documents

ProAgent V2.0 Public Edition


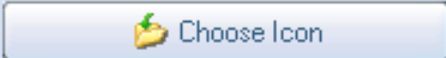
Send Menu

- ☒ Send Passwords
- ☒ Send CD-Keys
- ☒ Send KeyLog
- ☒ Send System Information
- ☒ Send Address Book
- ☒ Send URL History
- ☒ Send Processes Log

Options

- ☐ Give a fake error message
- ☐ Melt server on install
- ☒ Disable AntiVirus Programs
- ☒ Clear Windows XP Restore Points
- ☐ Protection for removing Local Server


Server Icon
You can choose any icon for server


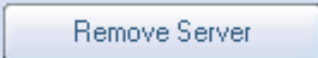
 




Bind with File
You can bind server with any files you want


☐ Bind with File 

Notification
Your e-mail address which you will to receive information from ProAgent.

E-Mail: 



ProAgent - Professional Agent Copyright © 2005 SIS-Team



Recycle Bin



ProAgent



9:56 AM

Spy Instructors Software

NEW GENERATION SOFTWARE SOLUTIONS



HOMEPAGE



PRODUCTS



DOWNLOADS



FORUMS



ABOUT US



ProAgent v2.1



- ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.
- It is an ultimate solution for monitoring spouses, children, employees, or anyone else!
- ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!
- ProAgent can work in all kind of networks, it doesn't matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase **ProAgent v2.1** Special Edition...

Click here to download **ProAgent v2.1** Public Edition

SIS - Products



Purchase Program



Customer Support Department



Commercial Programs



Freeware Programs



Custom Special Programs

New Generation Software Solutions...

New Products

SIS-IExploiter v2.0



ProAgent v2.1



AntiDote v1.2

SIS-Downloader

Virtual Keyboard

allBots Inc.

Social Networking Bots

GOOD News!!! We have something more for you! Yes, we have just integrated **CAPTCHA Bypasser** in all of our bots.

Winsock (Multi-threaded) Bots

Become an **Affiliate** and **Start Earning Now**

Click here for 30+ MySpace Bots

Accounts Creator

(You Just Need To Type In The CAPTCHAs To Create Accounts)

Social Networks

| | | | |
|---|---|---------------------|-----------------|
| MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager |  | \$180.95 | \$140.00 |
| MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock) |  | \$360.95 | \$320.00 |
| YouTube Accounts Creator |  | \$120.95 | \$95.00 |
| Friendster Accounts Creator |  | \$120.95 | \$95.00 |
| Hi5 Accounts Creator |  | \$120.95 | \$95.00 |
| TagWorld Accounts Creator |  | | |

Friend Adders, Message Senders, Comment Posters & Others

(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)

****Chaining Feature**** Is Available On All Bots for All Networks Except Facebook

Advertisement

i have boa wells and barclays bank logins....

have hacked hosts, mail lists, php mailer send to all inbox

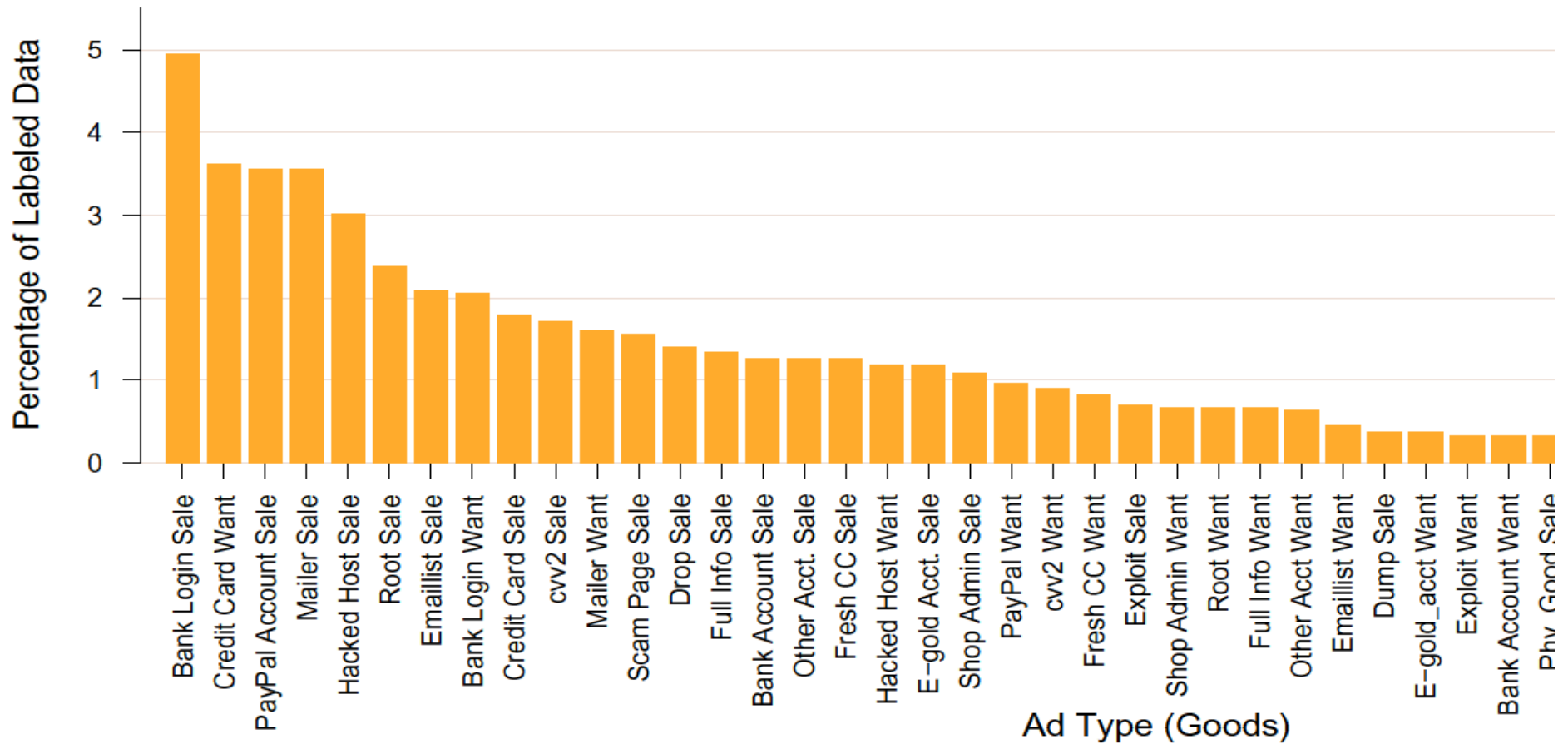
i need 1 mastercard i give 1 linux hacked root

i have verified paypal accounts with good balance...and i can cashout paypals

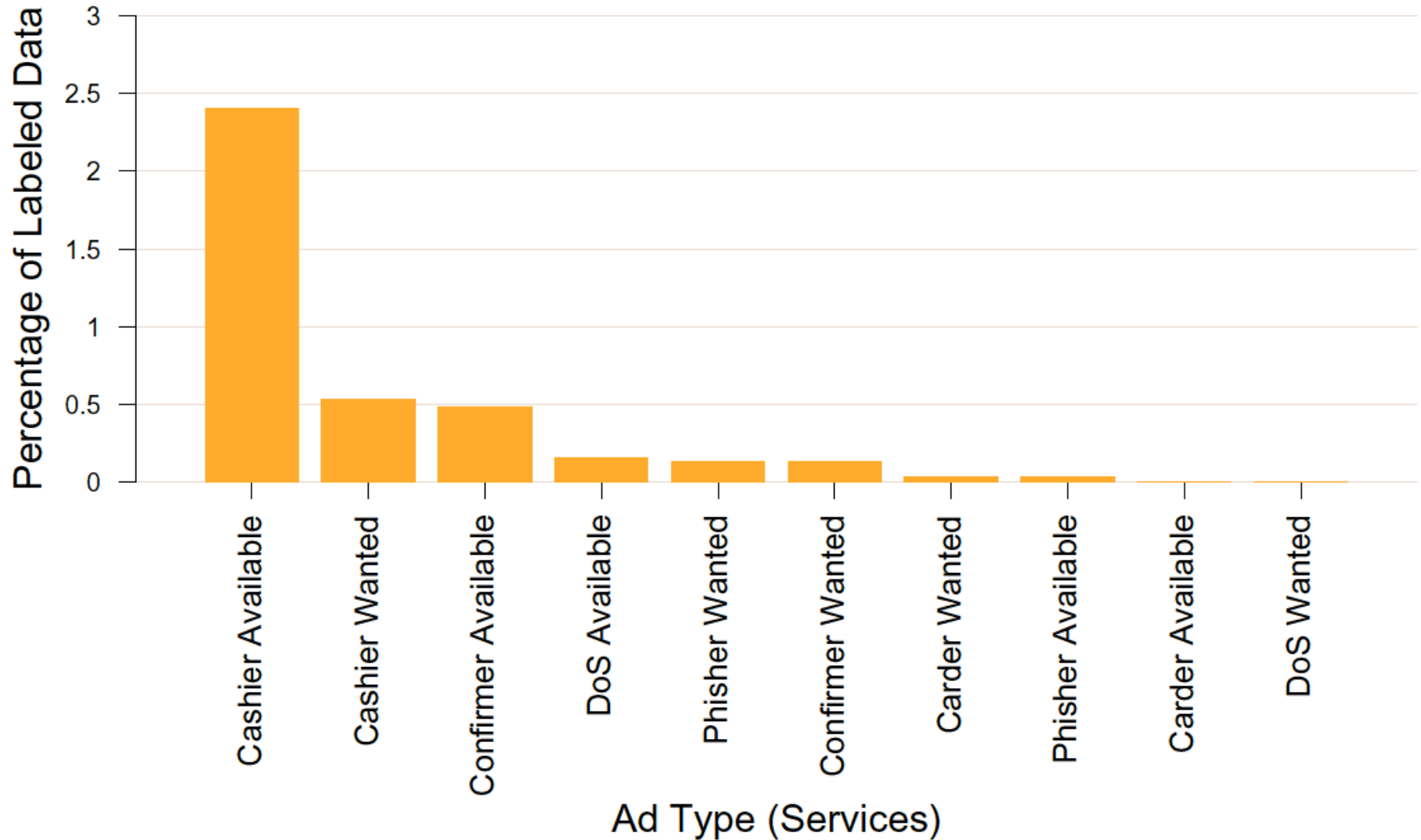
| | |
|--------|---------------------------------------|
| OrAcLe | I NEED INBOX MAILER ..HOW MUCH IS IT? |
| OrAcLe | i REQUIRE IT |
| <ehmo> | yop |
| OrAcLe | ? |
| OrAcLe | IS IT TO ALL INBOX? |
| <ehmo> | 5\$ |
| <ehmo> | hm |
| OrAcLe | WILL YOU PLS ACCEPT \$3 |
| <ehmo> | many people selling for 3 |
| <ehmo> | ask him |
| OrAcLe | WHO? |
| <ehmo> | dono |
| OrAcLe | hm? |
| OrAcLe | bRO...I REALLY WANNA BUY 4RM YOU |
| <ehmo> | ok |
| OrAcLe | Already uploaded i hope |
| <ehmo> | yes |
| OrAcLe | Ok..what's ur egold acct ? |
| <ehmo> | give me a second |
| OrAcLe | Ok..i wait |

| | |
|--------|---|
| OrAcLe | Ok..i wait |
| OrAcLe | Please make sure that it is the account that you intend to spend to. |
| OrAcLe | Amount: 5.00 US Dollars' worth of Gold |
| OrAcLe | From: [elided] (Anthrax De Oracle) |
| OrAcLe | Is this info correct? |
| OrAcLe | Ok..i send now |
| OrAcLe | e-metal. payment confirmation: Batch [elided] |
| OrAcLe | Paid To: [elided] (Filialka) |
| OrAcLe | Memo: |
| OrAcLe | |
| OrAcLe | Actual payment weight = 0.007704 oz. (0.239626 grams) |
| OrAcLe | Equivalent USD amount of this payment: \$5.00 |
| OrAcLe | Applicable Conversion factors: |
| OrAcLe | 1 oz. troy = 31.1034768 grams |
| OrAcLe | Gold exchange rate = 649.00USD/oz |
| OrAcLe | The e-metal payment was successful |
| OrAcLe | Your batch number for confirmation is [elided] |
| OrAcLe | Thank you for using e-gold. |
| OrAcLe | SENT |
| — — | I'm SELLING Usa AOL Fulls Info CC also - Uk/Eu Full info - with unique algo.. ! .5.Payment Only E-GOLD |

Marketplace Ads for Goods



Marketplace Ads for Services



September 6th, 2007

Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

Categories: [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox.....](#)

Tags: [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



150 TalkBacks

ADD YOUR OPINION



SHARE



PRINT



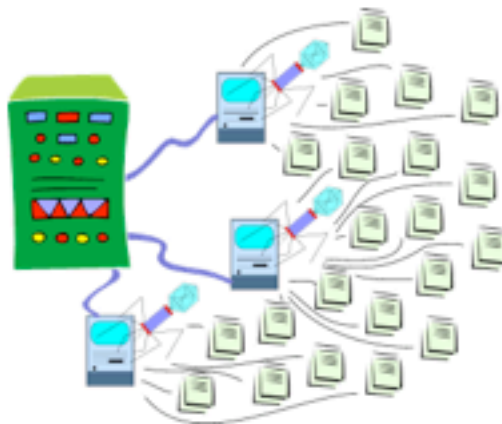
E-MAIL



+97

WORTHWHILE?

115 VOTES



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

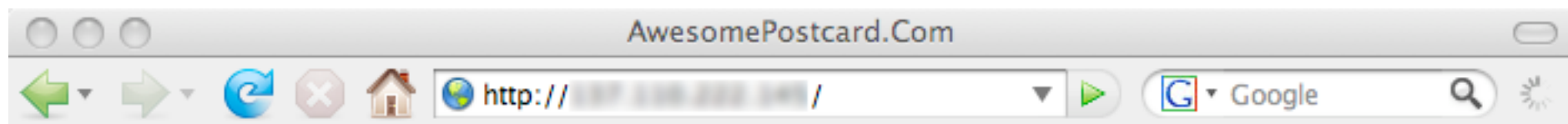
“

The [Storm] botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet, and is estimated to be capable of executing more instructions per second than some of the world's top supercomputers. However, it is not a completely accurate comparison, according to security analyst James Turner, who said that comparing a botnet to a supercomputer is like comparing an army of snipers to a nuclear weapon

If that made you catch your breath a bit, read on...

“

At certain points in time, the Storm worm used to spread the botnet has attempted to release hundreds or thousands of versions of itself onto the Internet, in a concentrated attempt to overwhelm the defenses of anti-virus and malware security firms. According to Joshua Corman, an IBM security researcher, "This is the first time that I can remember ever seeing researchers who were actually afraid of investigating an exploit."

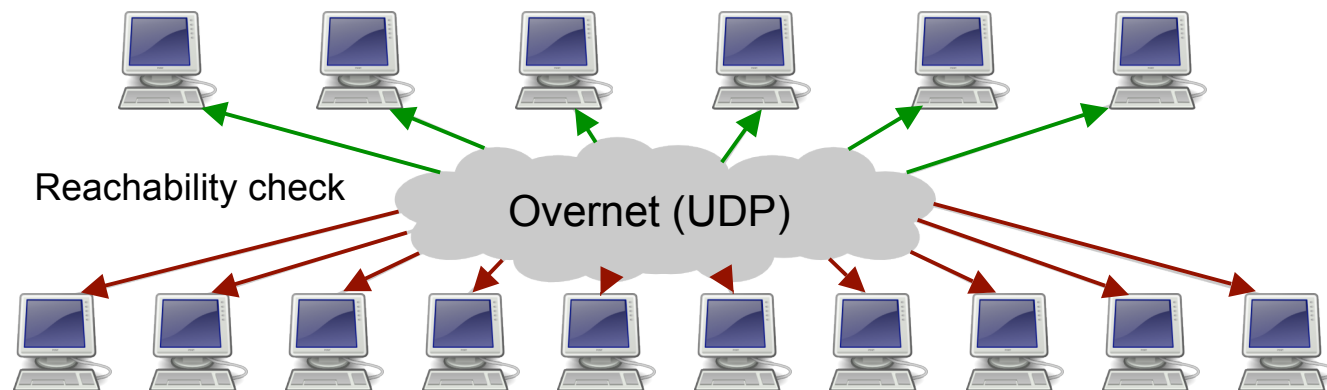


Your download will start in 5 seconds.
If your download does not start, [click here](#)

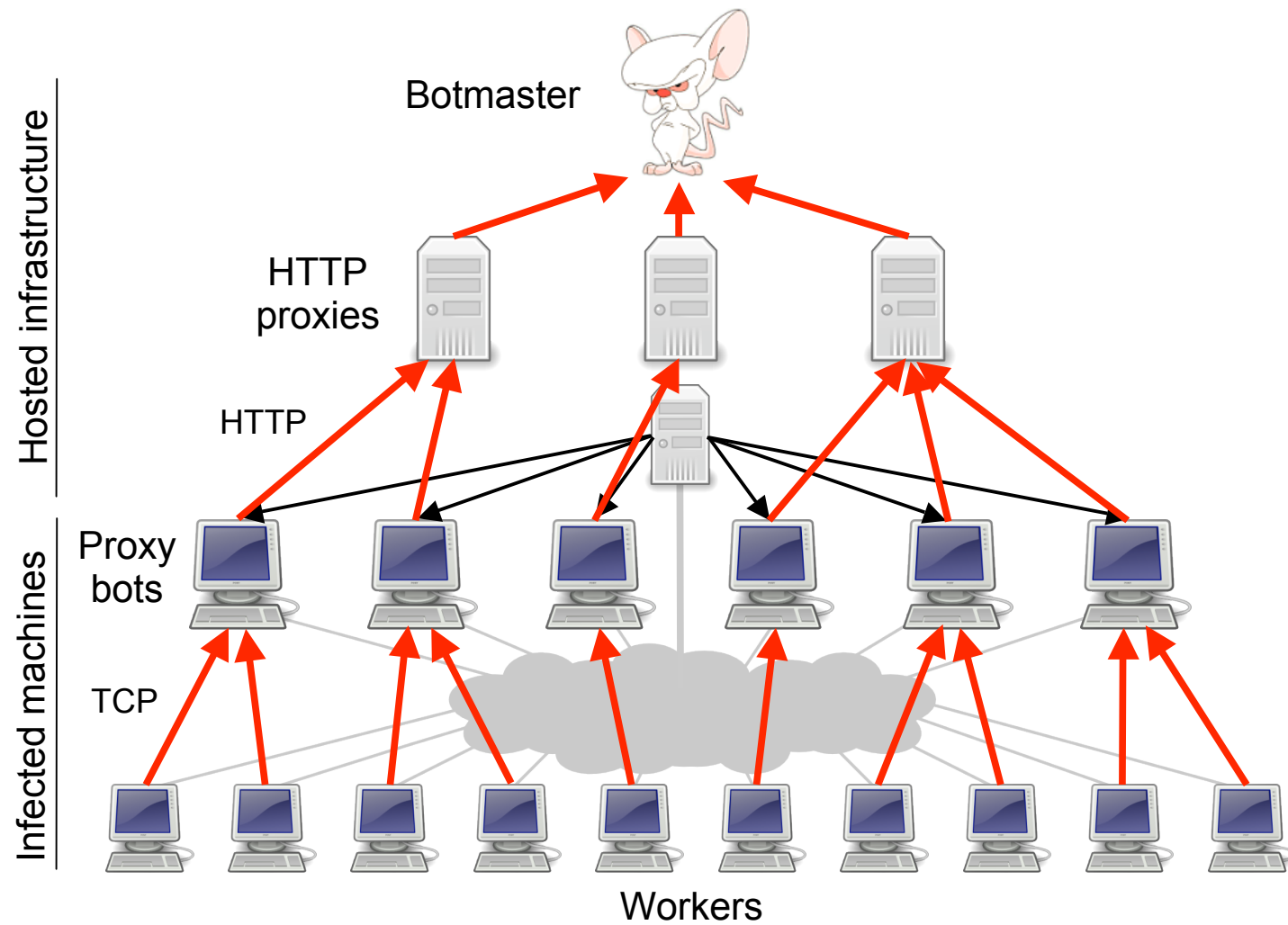
©2000-2008 AwesomePostCard.com - All rights reserved.

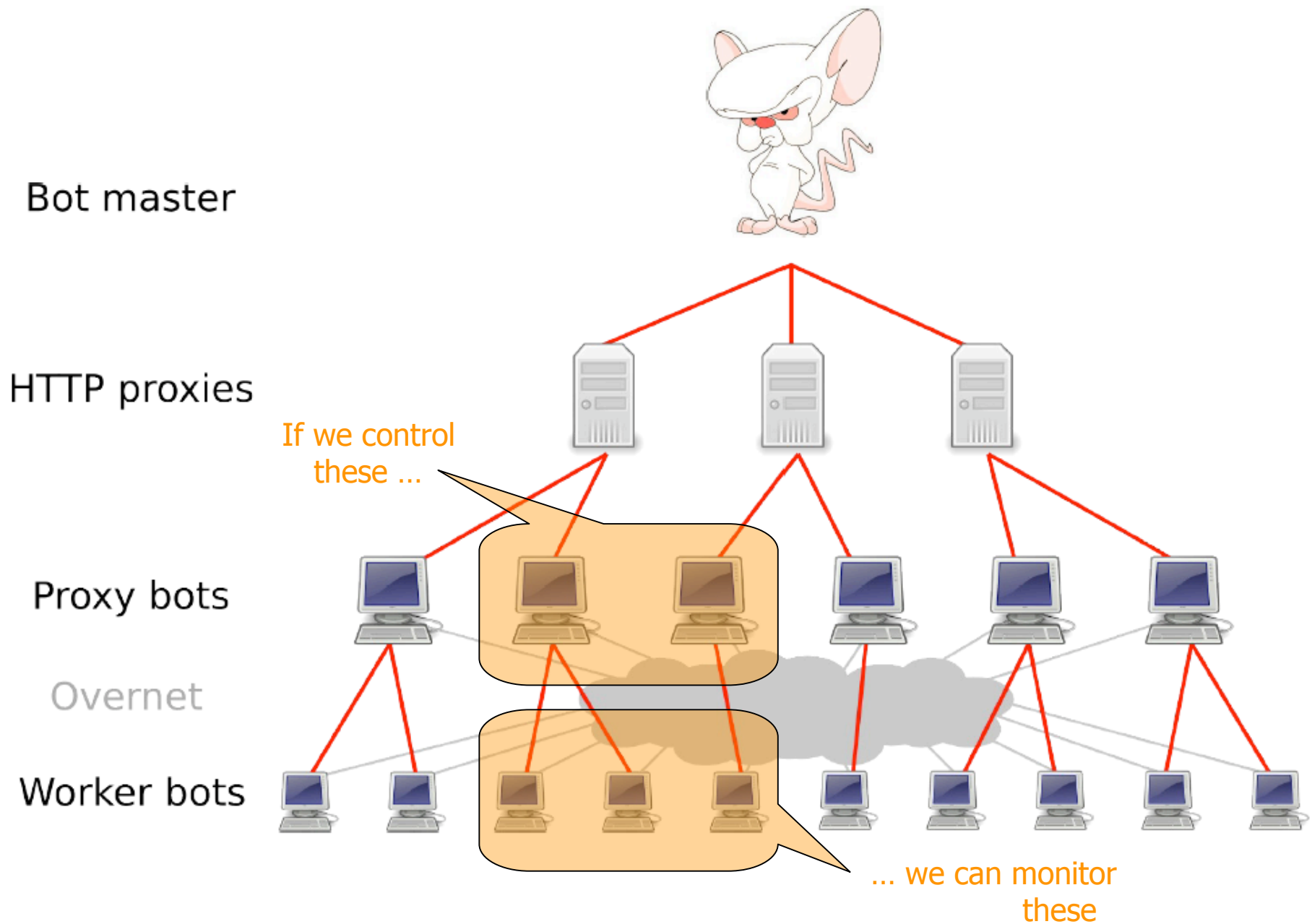
Done

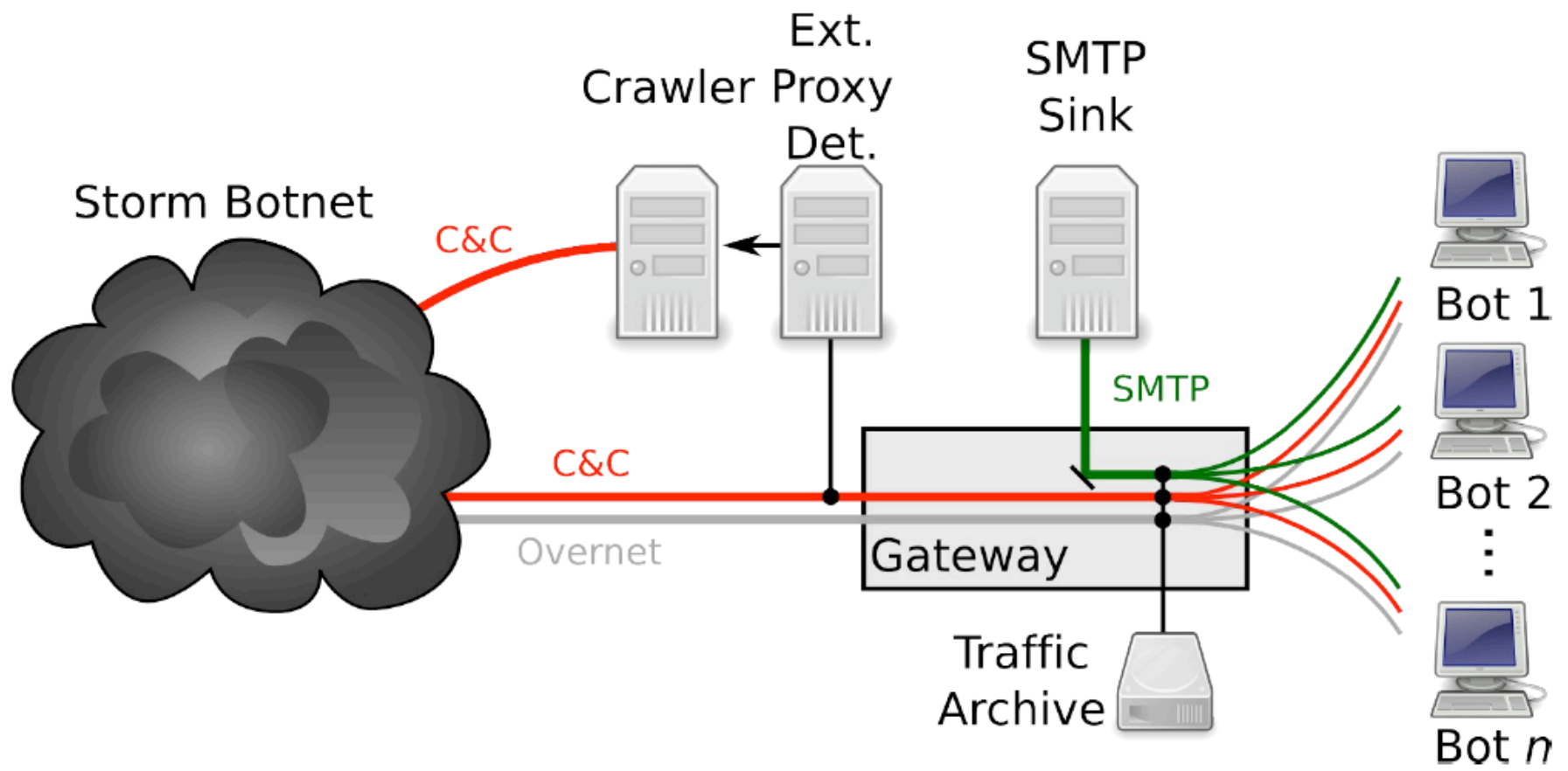
The Storm botnet



The Storm botnet







(PRNG). Storm generates OIDs using its own PRNG given by the recurrence:

$$I_{i+1} = (a \cdot I_i + b \bmod 2^{32}) \bmod m$$

with $a = 1664525$, $b = 1013904223$, $m = 32767$, and the initial value I_0 is based on the system clock. The generator appears to be based on a well-known linear congruential PRNG described in the *Numerical Recipes*

| Location | Hallmarks |
|----------------|---|
| Germany | Random OIDs with lower 10 bytes constant. Floods the Storm network aggressively with thousands of fake node IPs. |
| Iran | Random OIDs biased to upper half of space (first bit always set). |
| Sweden | Random OIDs biased to upper half of space (first bit always set). Does not appear in routing tables of any other peers. |
| France | One fixed OID, relatively passive crawler, appears to just be sampling Storm. |
| East Coast, US | 257 OIDs evenly distributed in ID space behind one IP, port number used as upper two bytes of the OID. |
| East Coast, US | Uniform random OIDs, both a Storm implementation and crawler behind the same IP, does not report other peers. |
| West Coast, US | Random OIDs biased to upper half of space 100:1. Does not report IPs in response to queries. |

Table 2: Other parties participating in the “encrypted” Storm network on April 4, 2008.

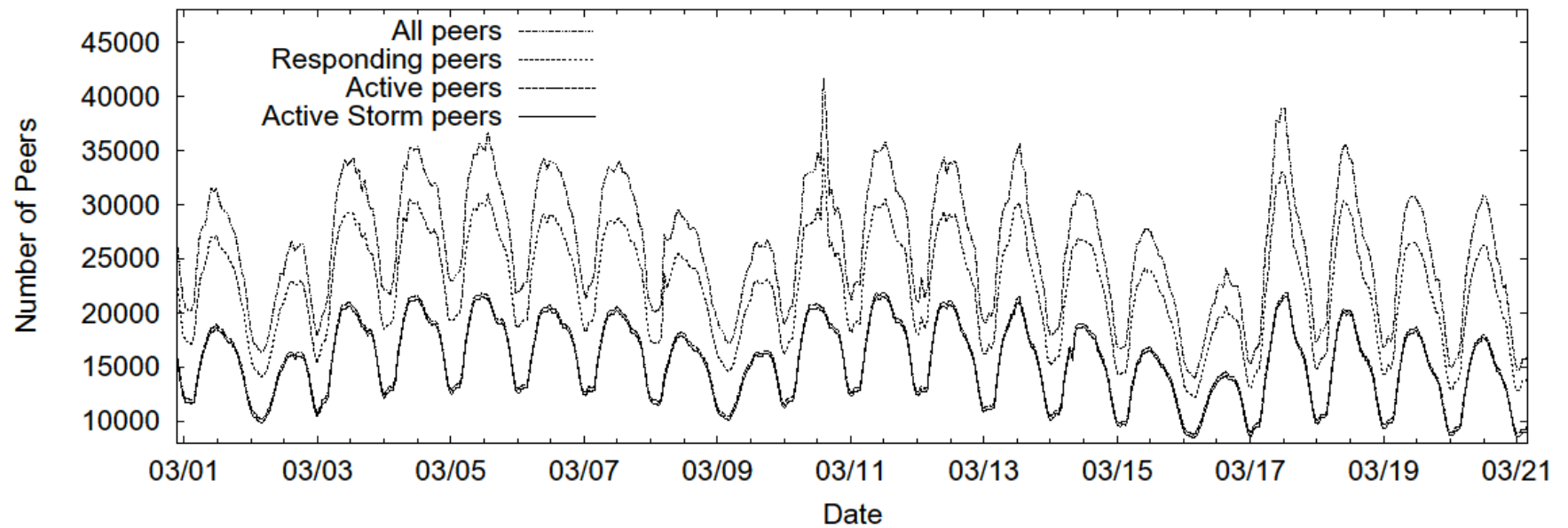
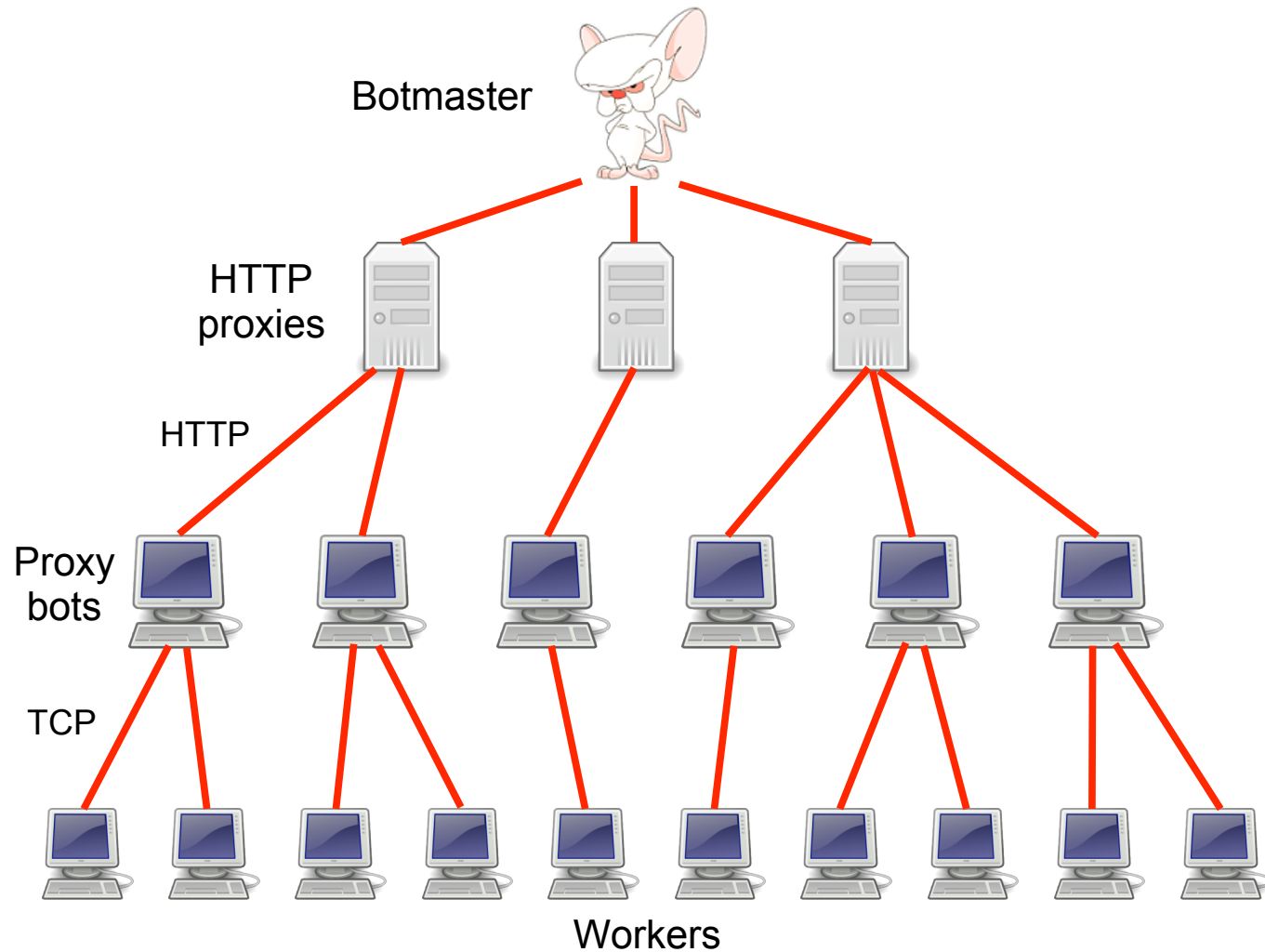


Figure 2: Estimates of the size of the Storm botnet using different notions of liveness over the first three weeks of March 2008
Note that the y -axis does not begin at zero to better separate the curves.

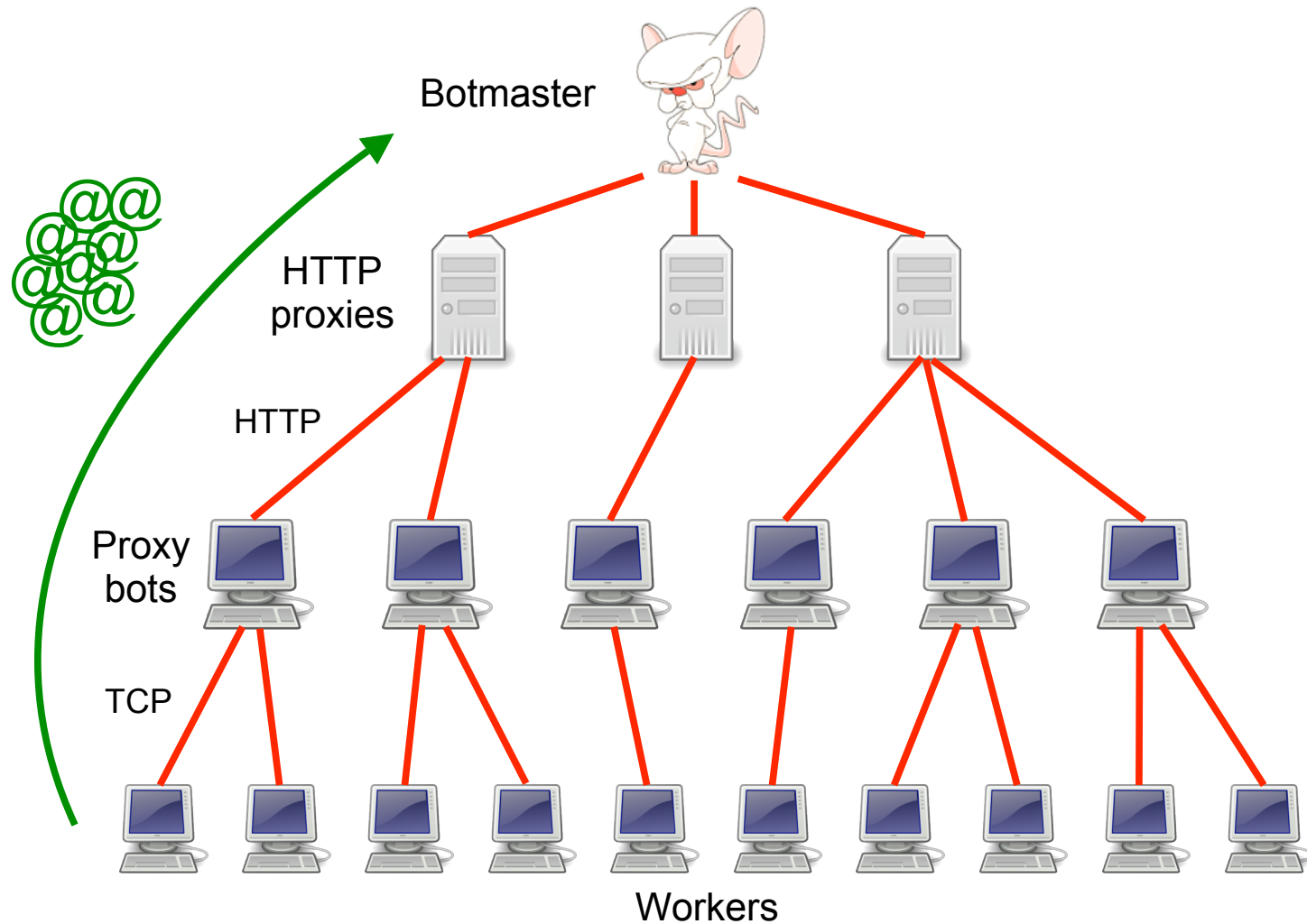
Types of Storm C&C Messages

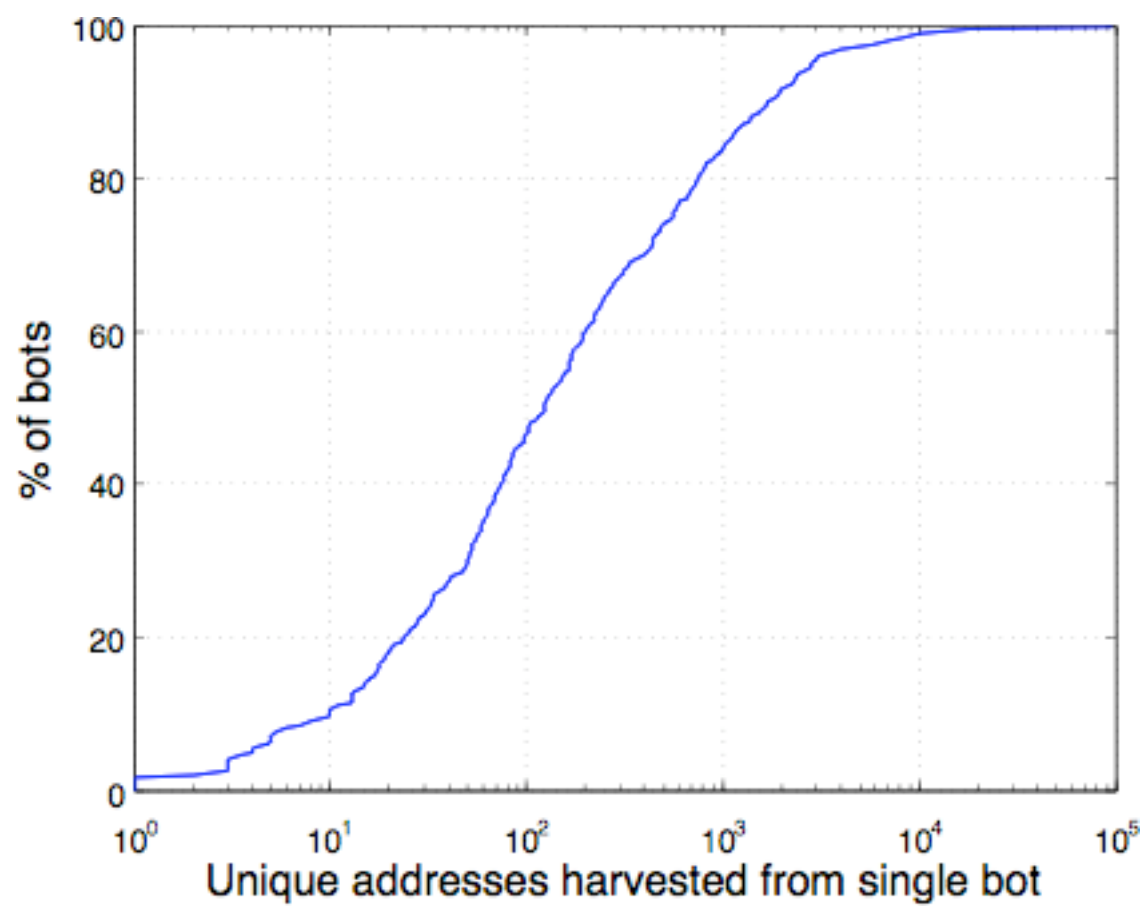
- Activation (report from bot to botmaster)
- Email address harvests
- Spamming instructions
- Delivery reports
- DDoS instructions
- FastFlux instructions
- HTTP proxy instructions
- Sniffed passwords report
- IFRAME injection/report

Spam campaign mechanics

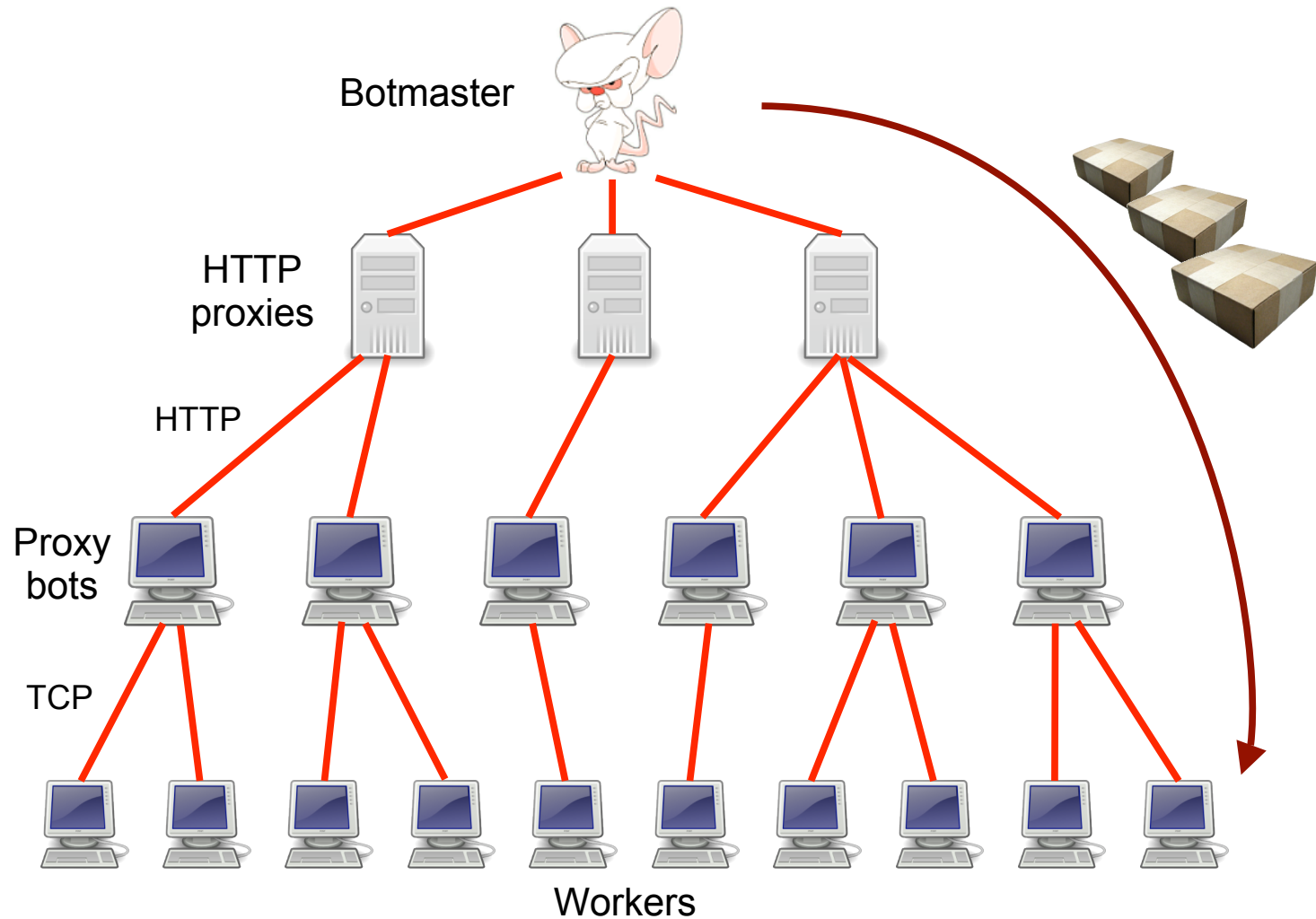


Campaign mechanics: harvest





Campaign mechanics: spamming



| MACRO | SEEN LIVE | FUNCTIONALITY |
|---|-----------|--|
| (O) | ✓ | 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. |
| (Cnum) | ✓ | 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. |
| (Fstring) | ✓ | Random value from the dictionary named <i>string</i> . ² |
| (Gstring) | ✓ | Line-wrap <i>string</i> into 72 characters per line. |
| (Hstring) | | 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. |
| (Jstring) | | 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. |
| (Ostring:num) | ✓ | Randomized message identifier element compatible with Microsoft SMTPSVC. |
| (Pnum ₁ [-num ₂]:string) | ✓ | Random string of <i>num</i> ₁ (up to <i>num</i> ₂ , if provided) characters taken from <i>string</i> . |
| (Qstring) | | Quoted-printable “=” linewrapping. |
| (Rnum ₁ -num ₂) | ✓ | Random number between <i>num</i> ₁ and <i>num</i> ₂ . Note, special-cased when used with (D). |
| (Ustring) | | Randomized percent-encoding of <i>string</i> . |
| (Vnum) | ✓ | Inserts the value of the field identified by (Cnum). |
| (W) | | Time and date as plain numbers, e.g. “20080225190434”. |
| (X) | | Previously selected member of the “names” dictionary. |
| (Ynum) | ✓ | 8-character alphanumeric string, compatible with Sendmail message identifiers. |
| (Z) | ✓ | Another Sendmail-compatible generator for message identifiers. |

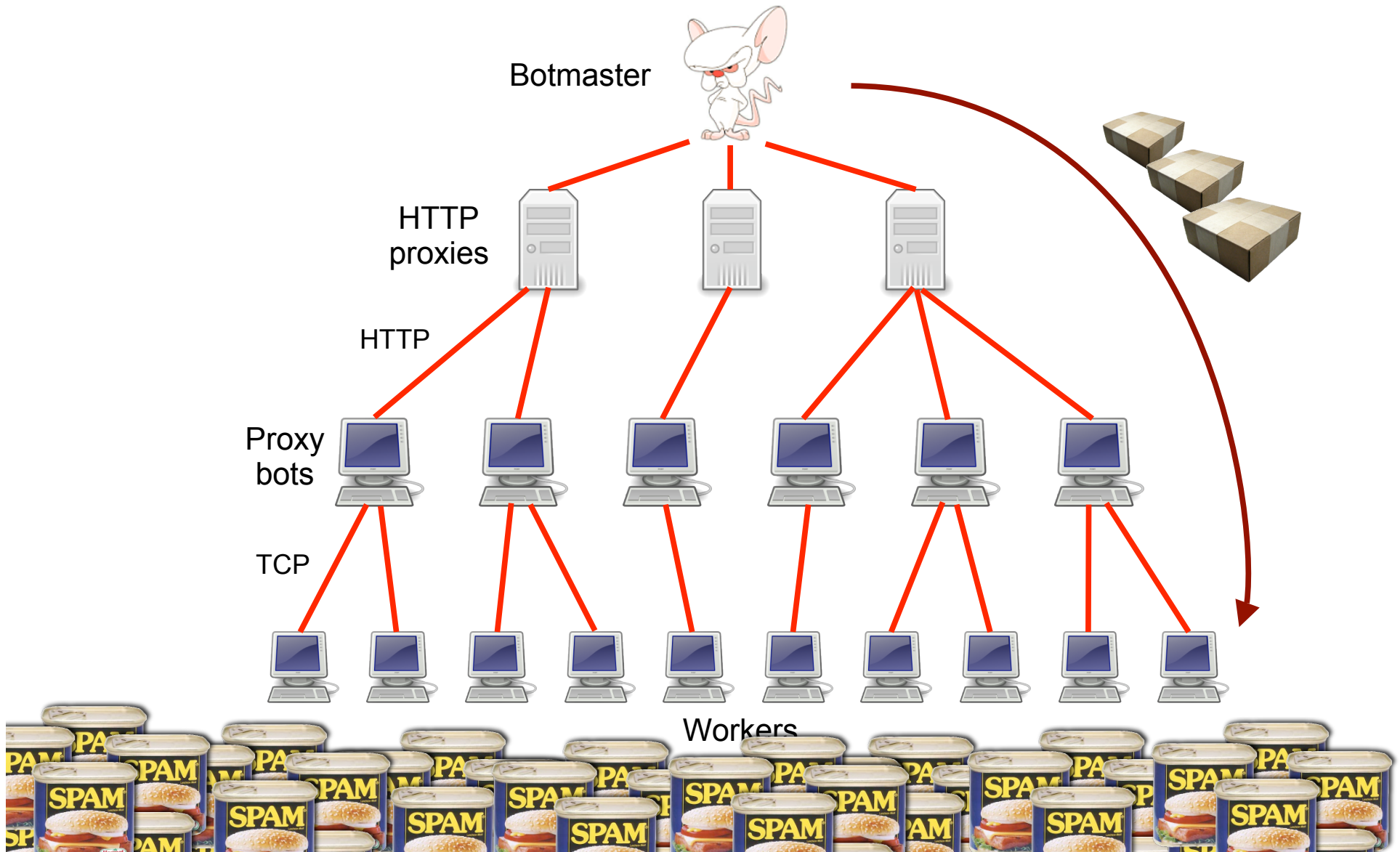
Table 2: Storm's spam-generation templating language.

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 | Attempts 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 supposedly 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 |

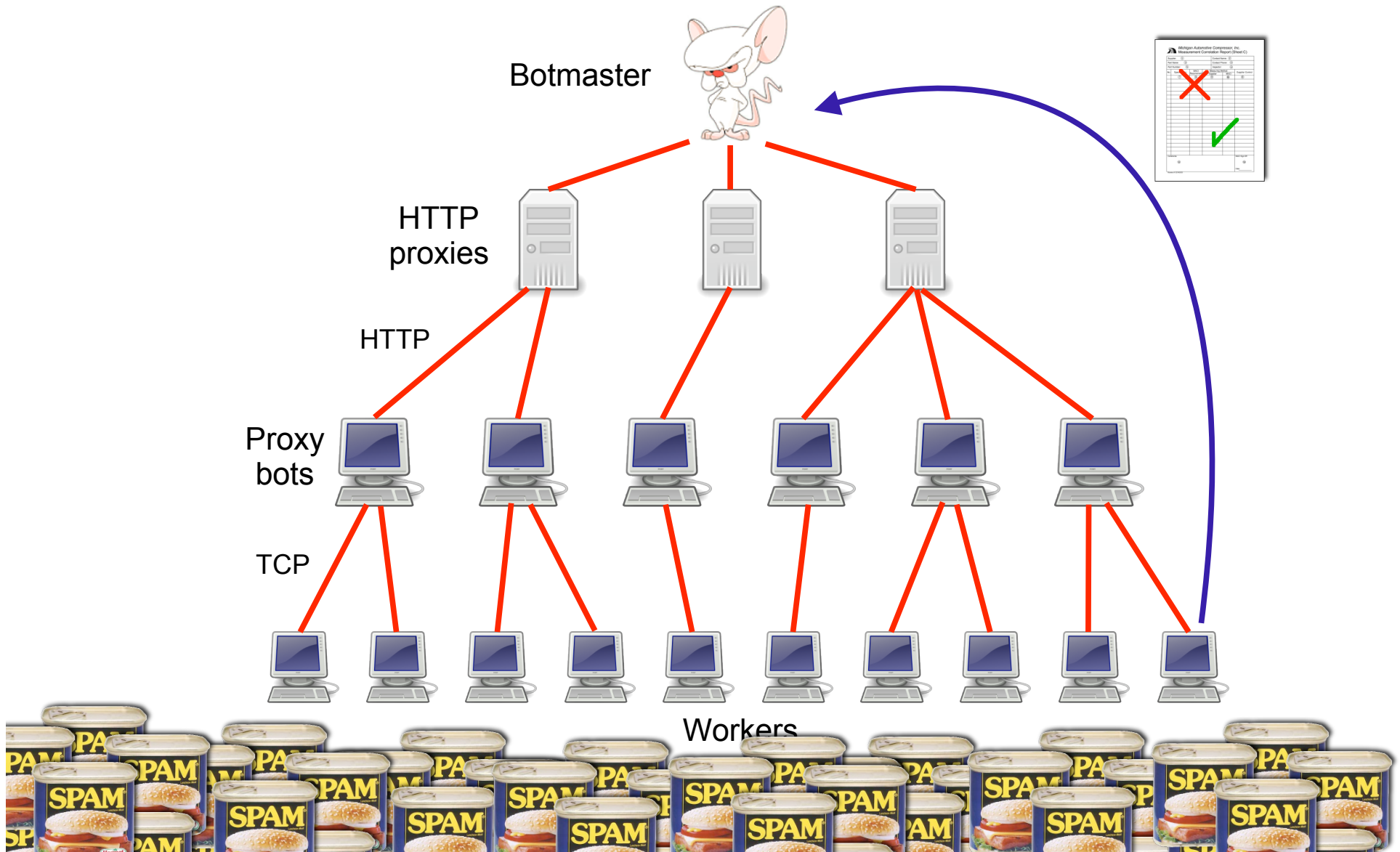
Table 3: Meanings of campaign classes.

Who is targeted?

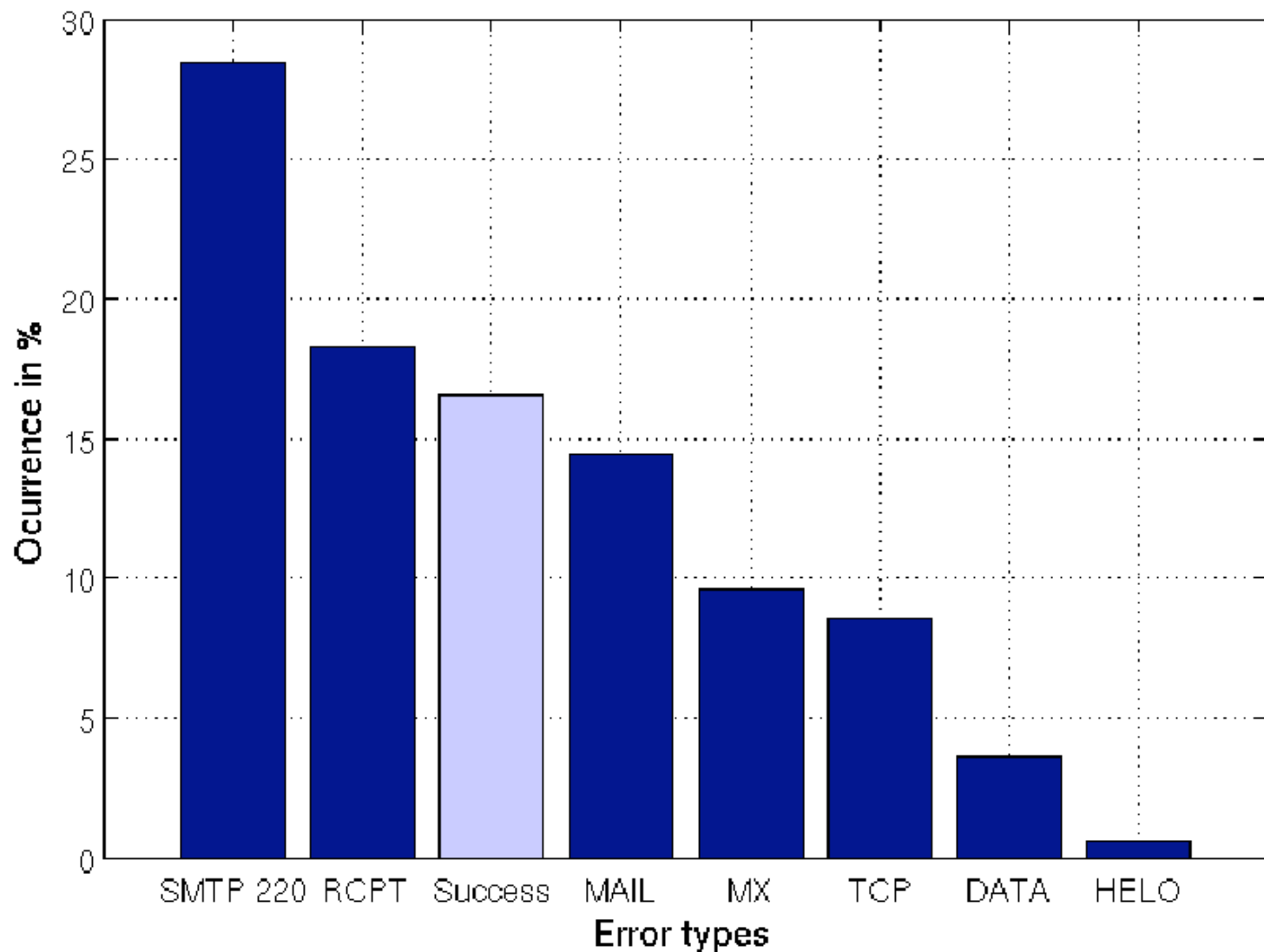
- **Top 20 domains**
 - Many Web mail & broadband providers, but very long tail
- **Campaigns have nearly identical distributions**
 - Same scammers, or target lists sold to multiple scammers
- Also see spam campaigns sent solely to *test accounts*

| 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



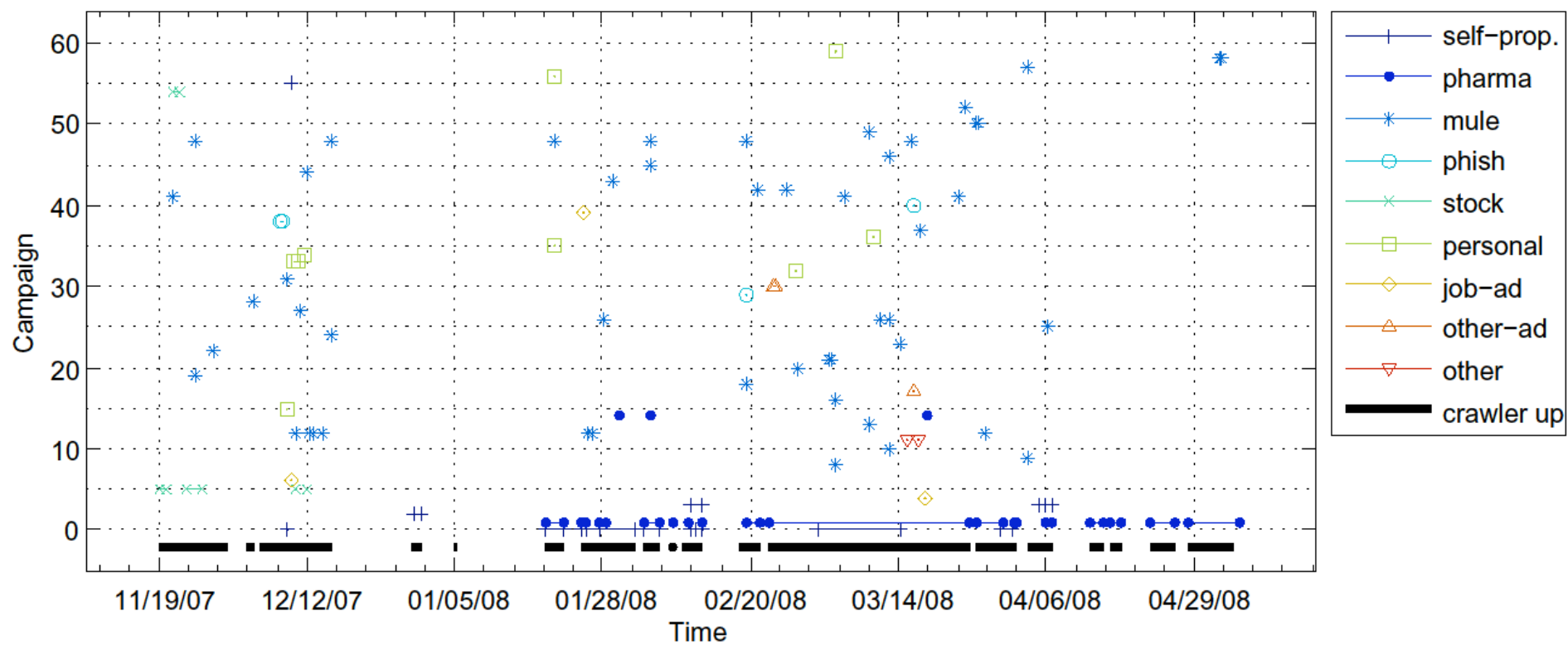


Figure 5: Classes and instances of spamming campaigns identified over time.

