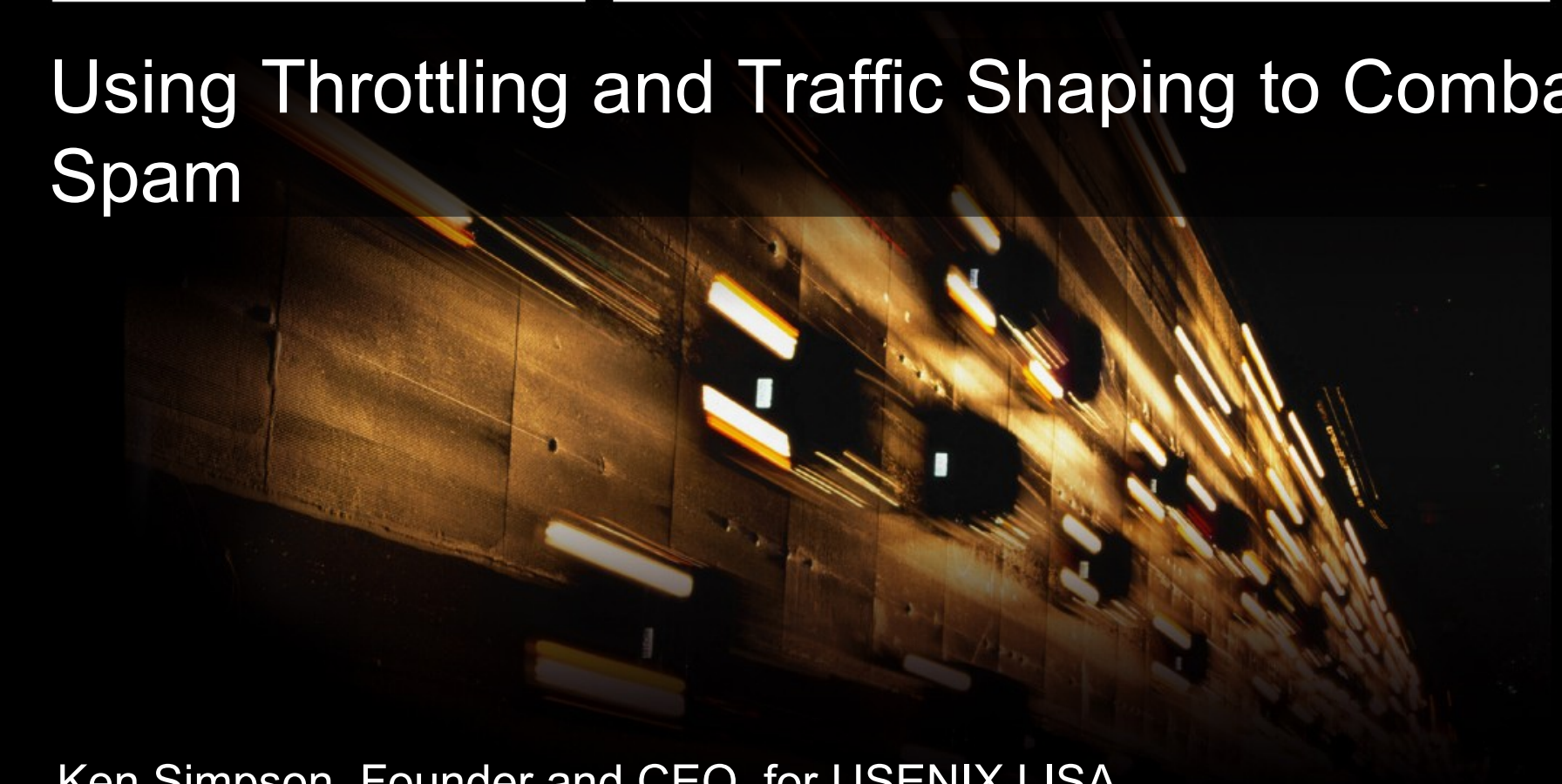
MAILCHANNELS

Using Throttling and Traffic Shaping to Combat Spam



Ken Simpson, Founder and CEO, for USENIX LISA

November 14, 2007

MAILCHANNELS

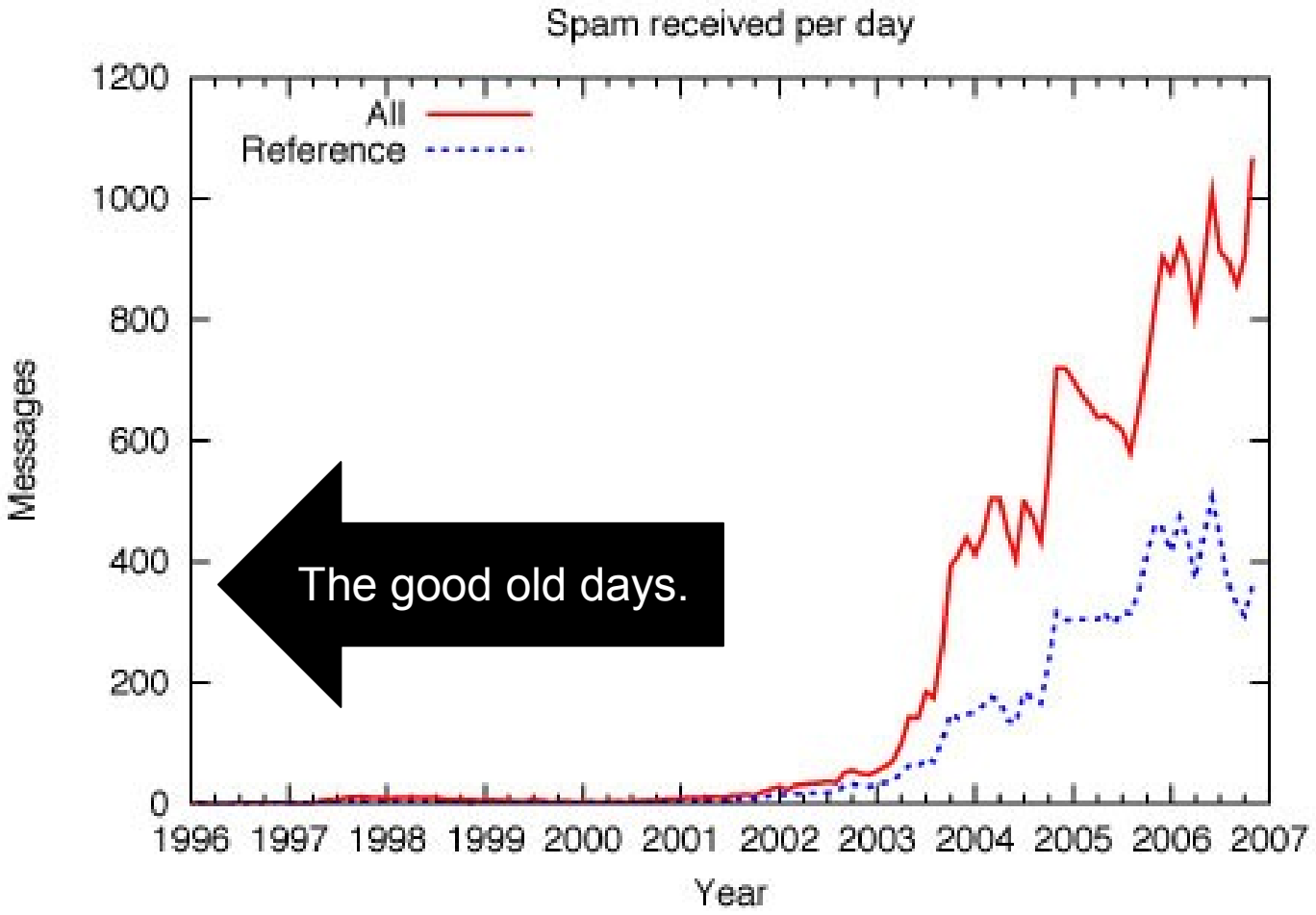
Overview

1. Spammus Historicum
2. Spammus Economicus
3. Spammus Interruptus
4. Question & Answer

- Beer & Spam at 8:30pm
  Room: “Reunion G”

MAILCHANNELS

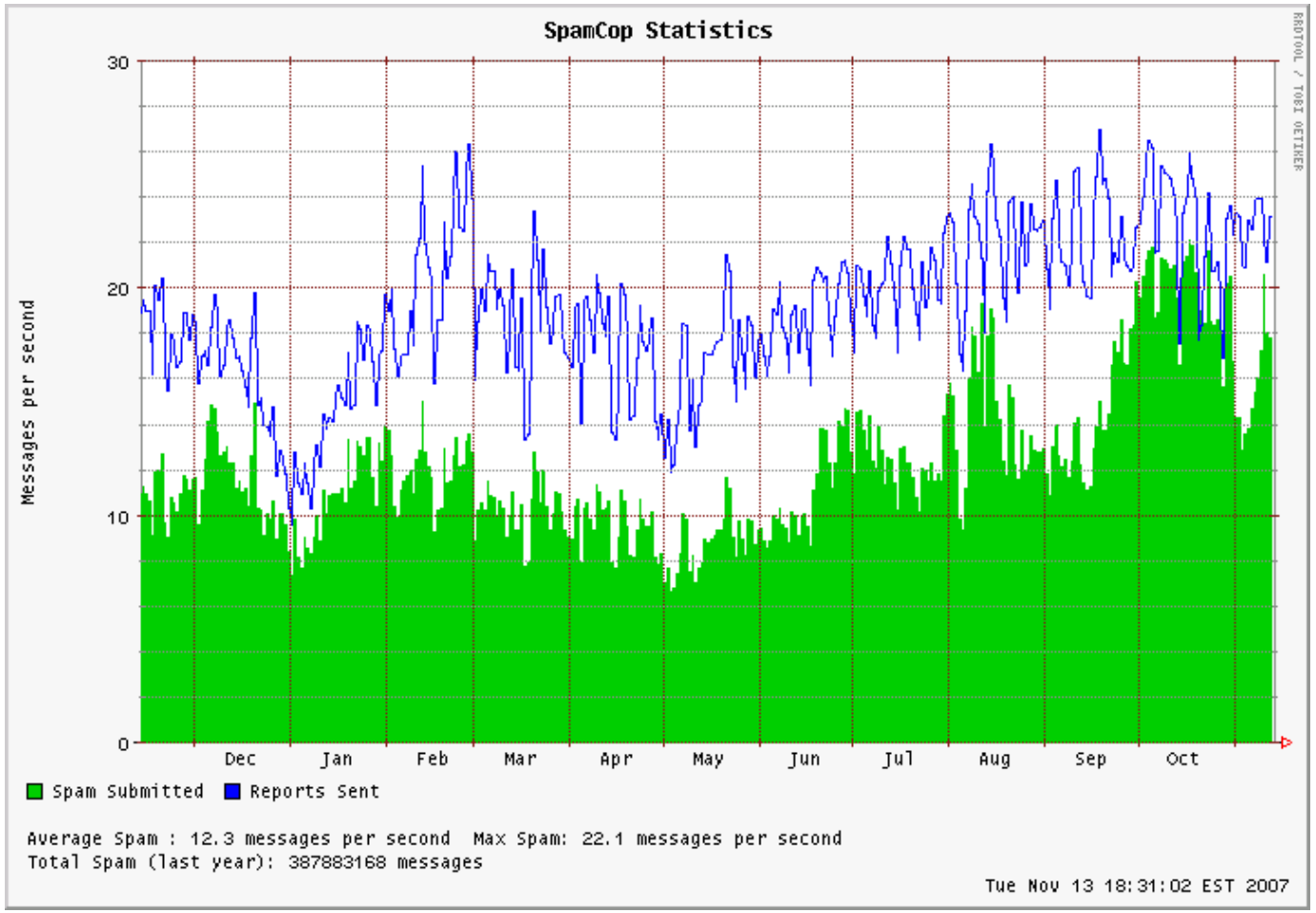
Spam: A Personal History



Source: spamnation.info/stats

MAILCHANNELS

Spam: A Personal History



MAILCHANNELS

The Dawn of Spam

- First spam was sent in 1978
- DEC marketing department advertising a seminar in California
  - Has anything really changed?

MAILCHANNELS

Spam Circa 2002

- Not much criminality yet
- Spamming still legal in most places
- First regex filters introduced
- **Attack**:
  - Simplistic shrouding of words
  - v1agra, c1al1s
- **Response**: Smarter regular expressions, and weighted rule sets.

MAILCHANNELS

Spam Circa 2003

- CAN-SPAM makes spamming illegal
- Some spammers move underground, others become “email marketers”
- Volume explodes
- **Attack**: Try hiding in fancy HTML.

```
<html><img src="http://www.your-info-station.com/Sla/chalkboard.gif
   "><div><ahref="http://www.your-info-station.com/Sla/eb.php?
   x=52c"><img src="http://www.your-info-
   station.com/Sla/pitch.gif"></a></html>
```

- **Response**: Filter on URLs, not words. Introduce Bayesian filtering. Blacklists.

MAILCHANNELS

Spam Circa 2004

- Bill Gates predicts spam will be gone in two years
- **Attack:**
  - Switch to botnets
- **Response:**
  - Improve reputation systems
  - Build enormous spamtraps
  - Implement greylisting

MAILCHANNELS

Spam Circa 2005-Present

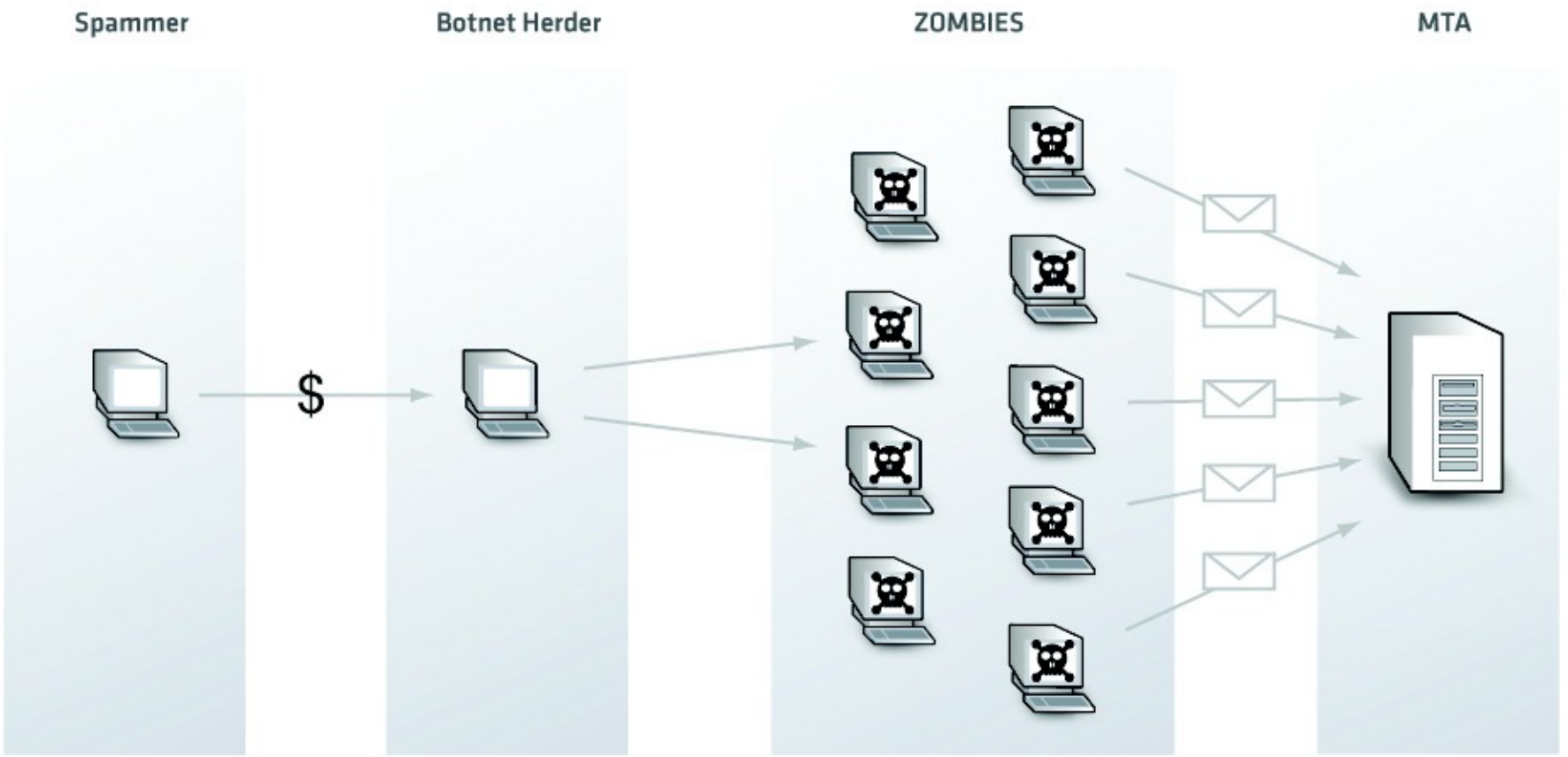
- **Attacks**:
  - Poison statistical filters
  - Hire full-time virus writers
  - Diversify into phishing and identity theft
  - Work with the mafia on stock spam
  - Rinse and repeat
- **Responses:**
  - Fingerprint-based filters

MAILCHANNELS

Spammer Economics

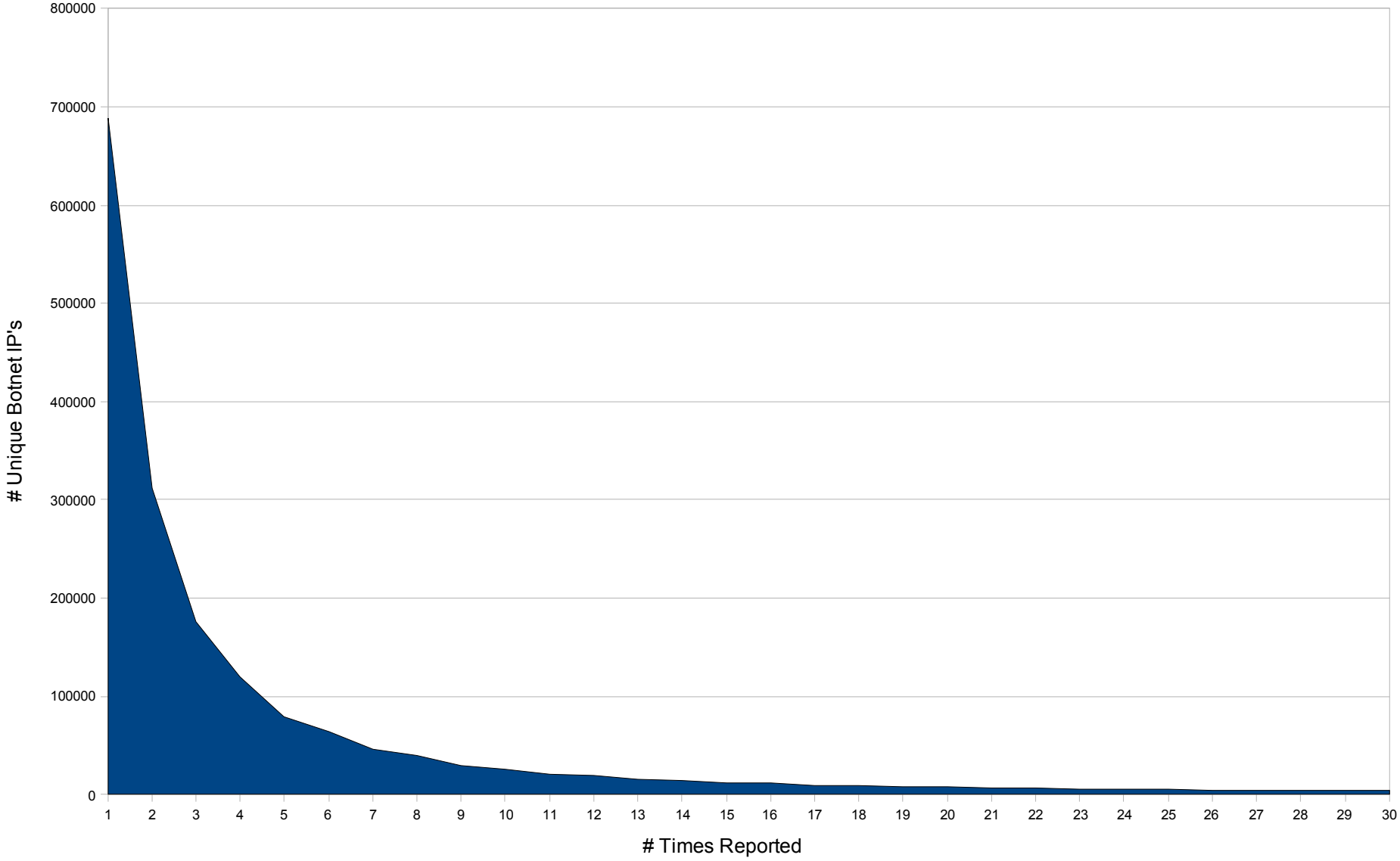
- Average filter accuracy is 90%
  - 1/10 of spam messages get through
- Improve accuracy to 95%
  - 1/20 of spam messages get through
- Solution?
  - Double spam volume
  - Same profit

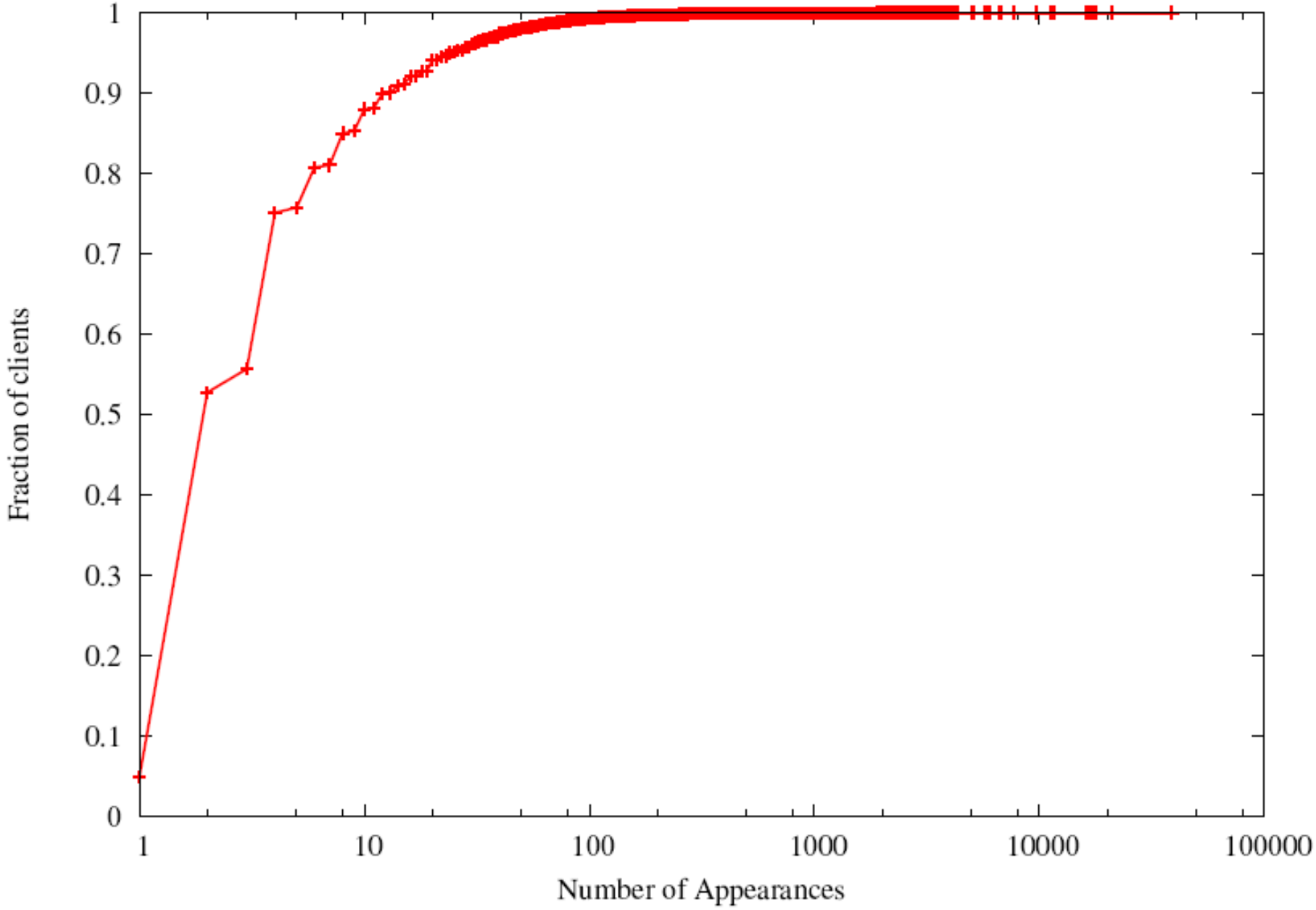
Botnet Architecture



How often do we see a unique Botnet IP?

The Number of Unique IP's versus the number of times reported



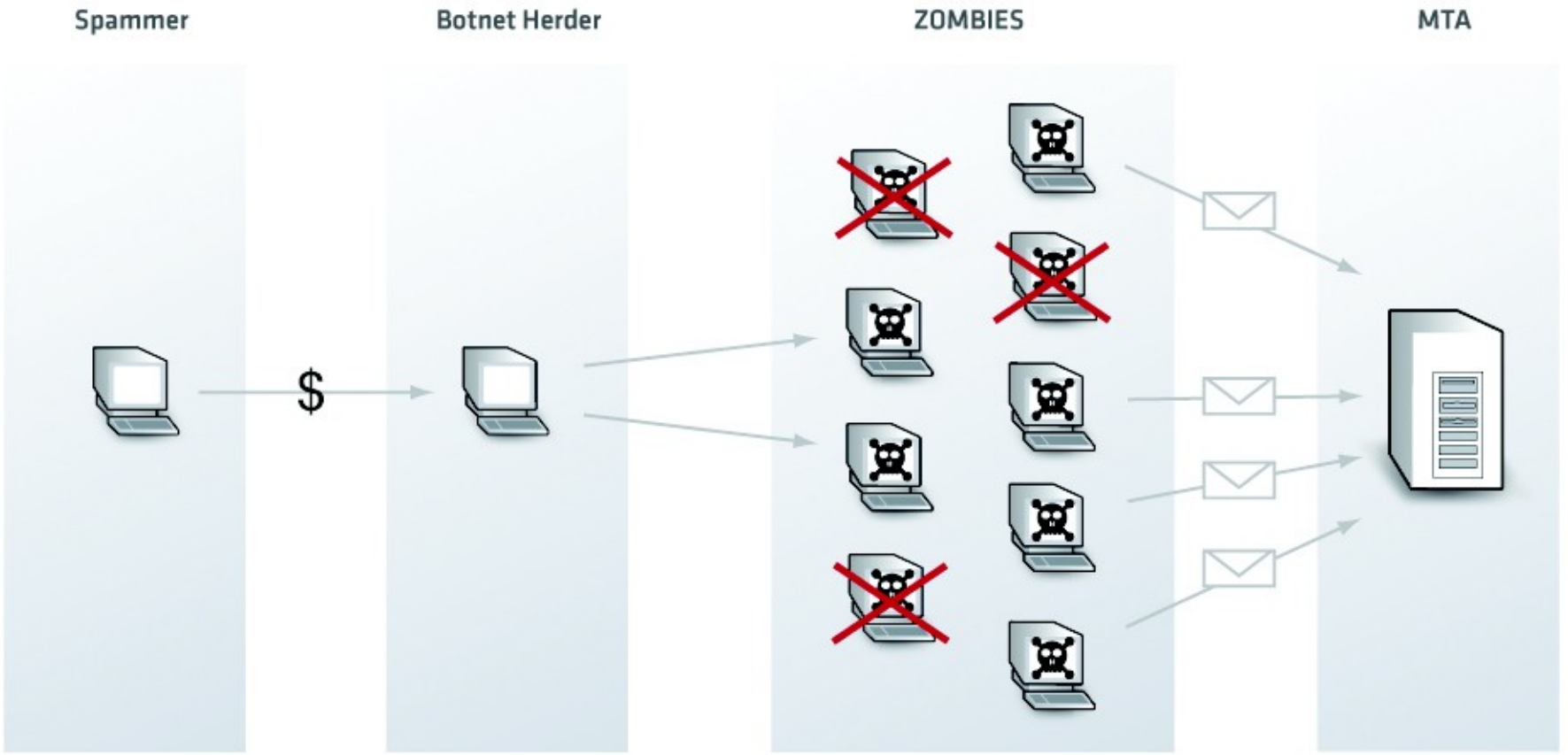

Fraction of clients
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1
10
100
1000
10000
100000
Number of Appearances

MAILCHANNELS

Zombies are Fickle

- 201.21.174.207
  - RBLs did not block this sender until it had sent 55 emails over 19 days.
  - All 55 were “rejected” by throttling.
  - After the RBLs caught up, a further 379 messages were received over 13 days

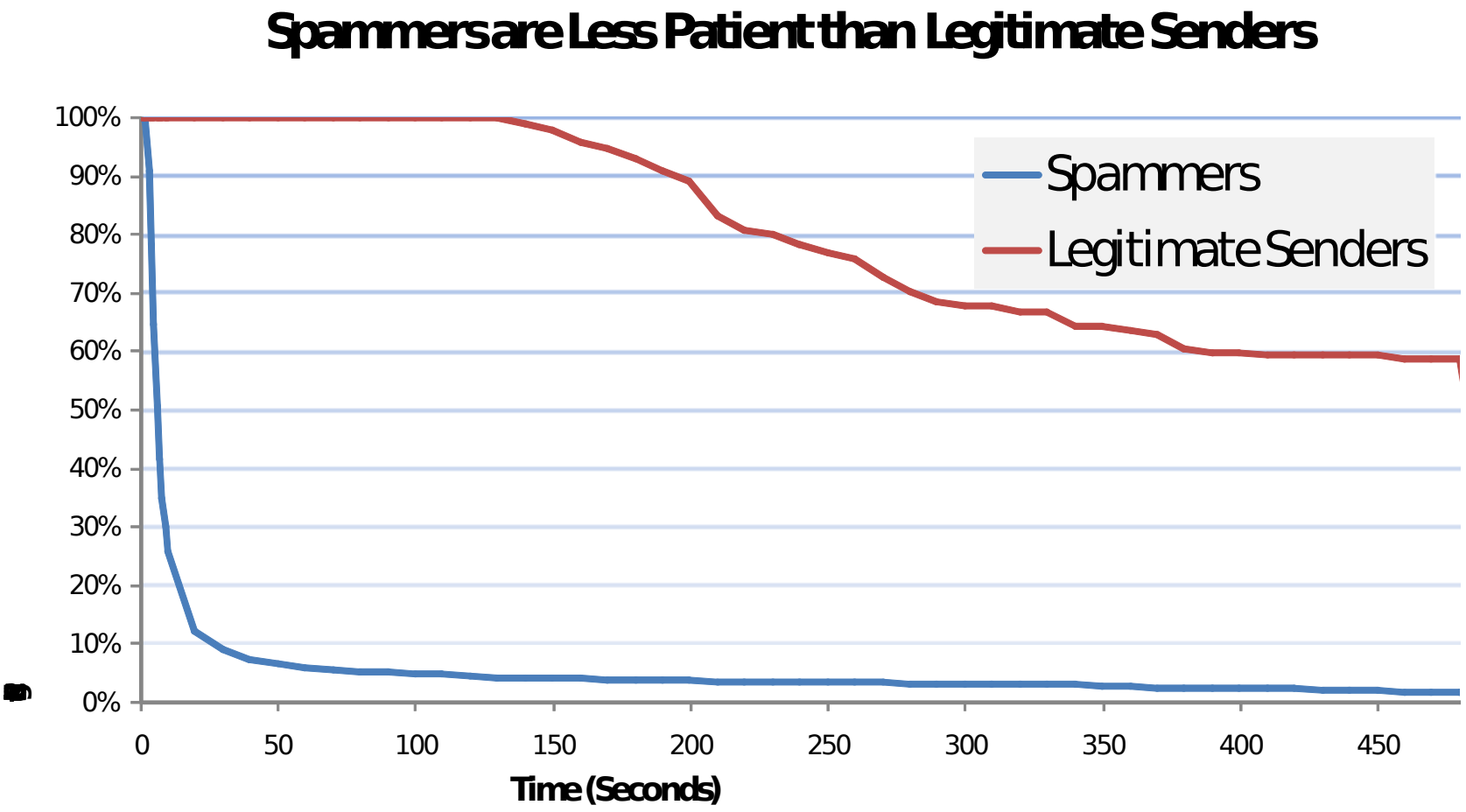
Botnet Architecture



MAILCHANNELS

Getting Paid

- EHLO foo.com
- *250 Ok*
- MAIL From: <bar@baz.com>
- *250 Ok*
- RCPT To: <victim@example.com>
- *250 Ok*
- DATA
- *354 Go ahead*
- ...
- *250 Queued* – ***Now I make some money***


Spammers are Less Patient than Legitimate Senders
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
0
50
100
150
200
250
300
350
400
450
Time (Seconds)
Spammers
Legitimate Senders

MAILCHANNELS

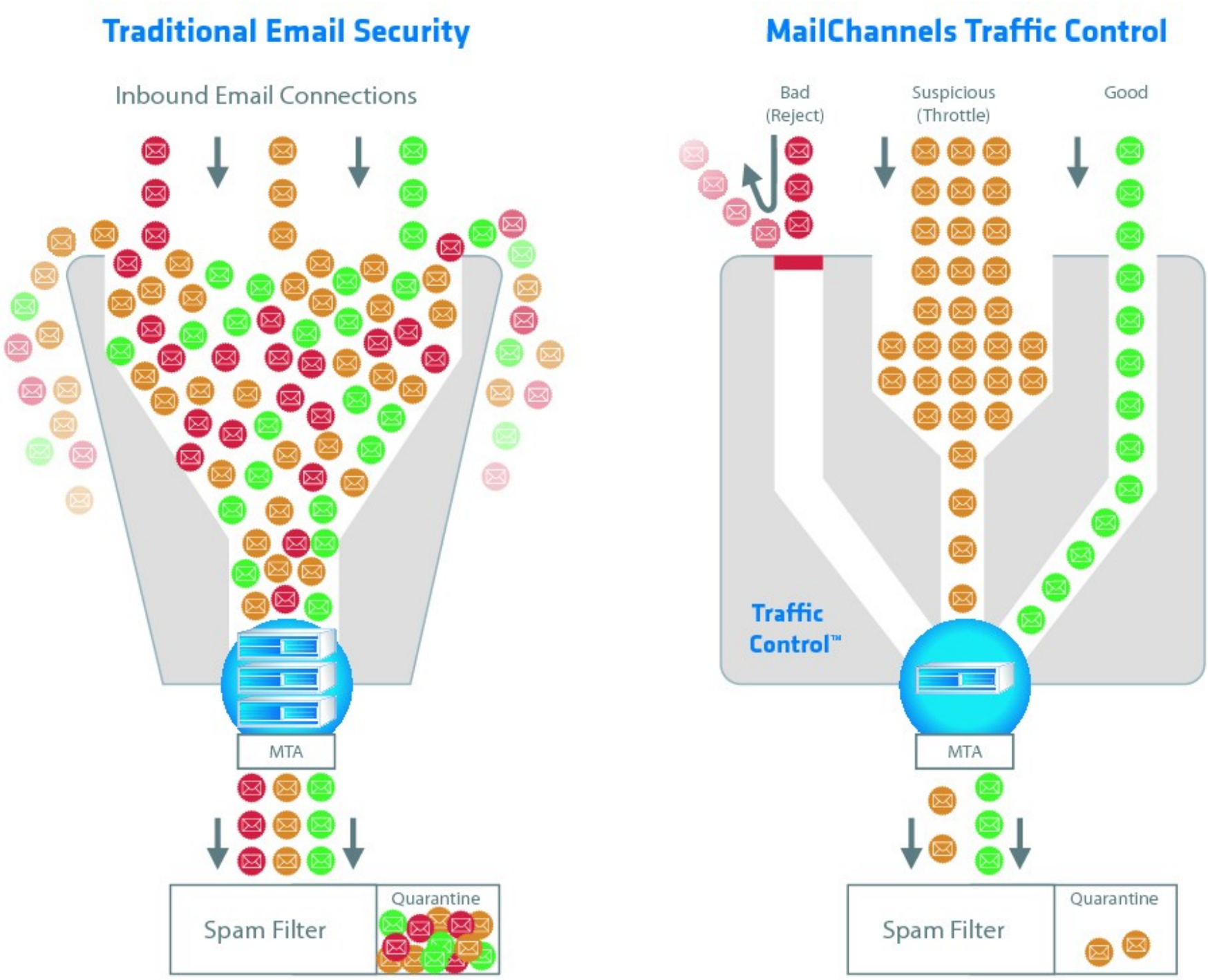
Intermission

- Improving filters is **hard**
- Identifying zombies is **hard**
- **What can we do?**

MAILCHANNELS

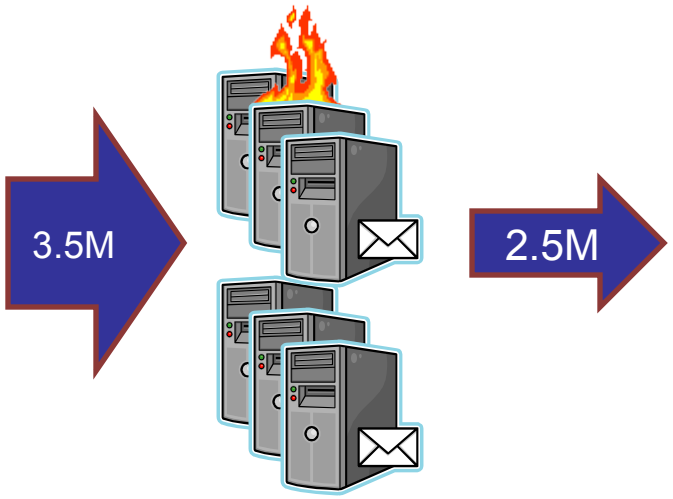
Idea

- **What can we do?**
- Attack the economics of the botnet.


Traditional Email Security
Inbound Email Connections
MTA
Spam Filter
Quarantine
MailChannels Traffic Control
Bad
(Reject)
Suspicious
(Throttle)
Good
Traffic
Control™
MTA
Spam Filter
Quarantine

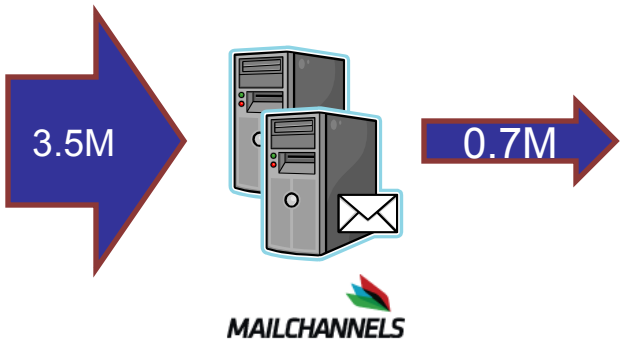
Case Study

October, 2006
Before Traffic Control

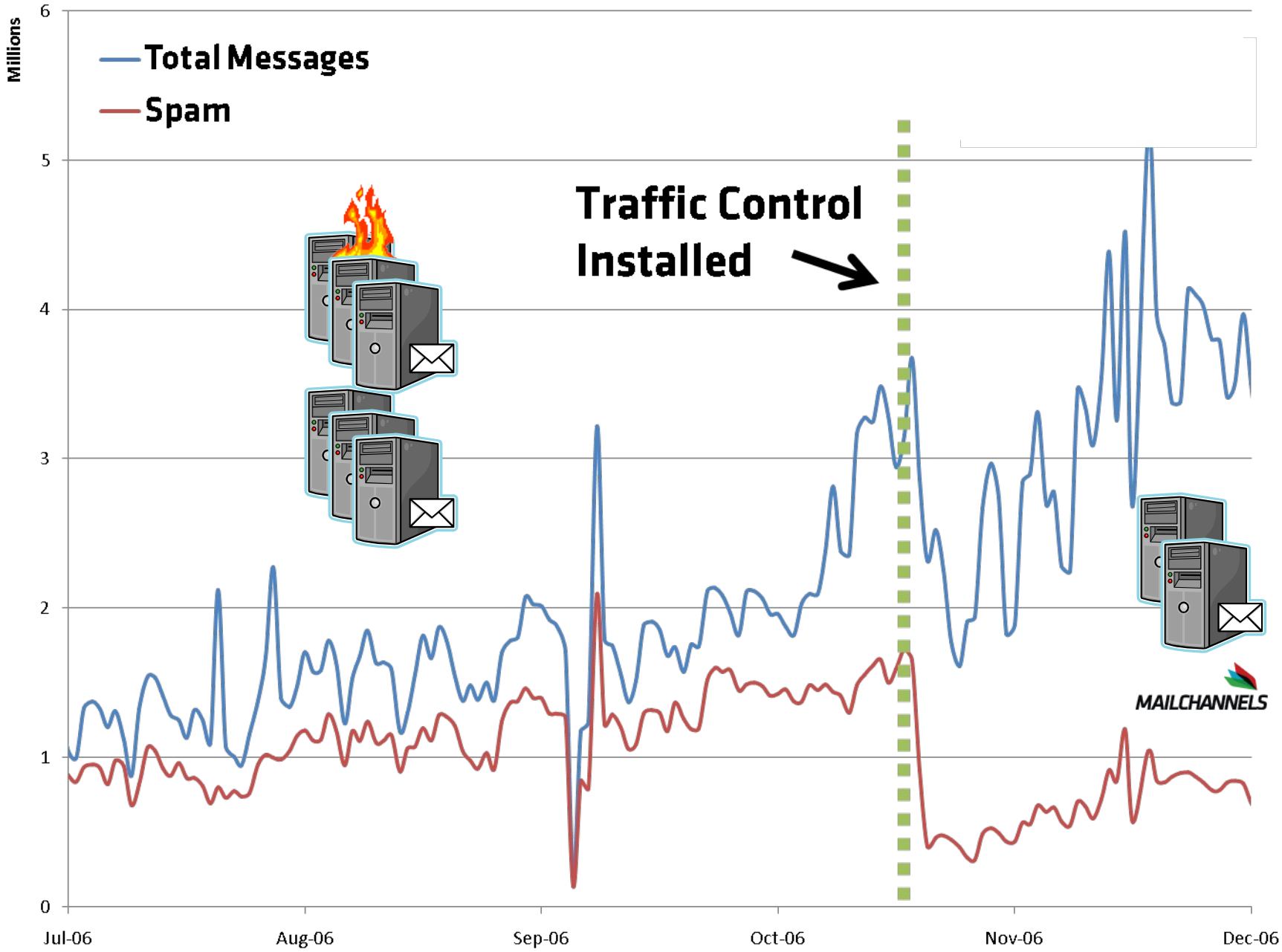


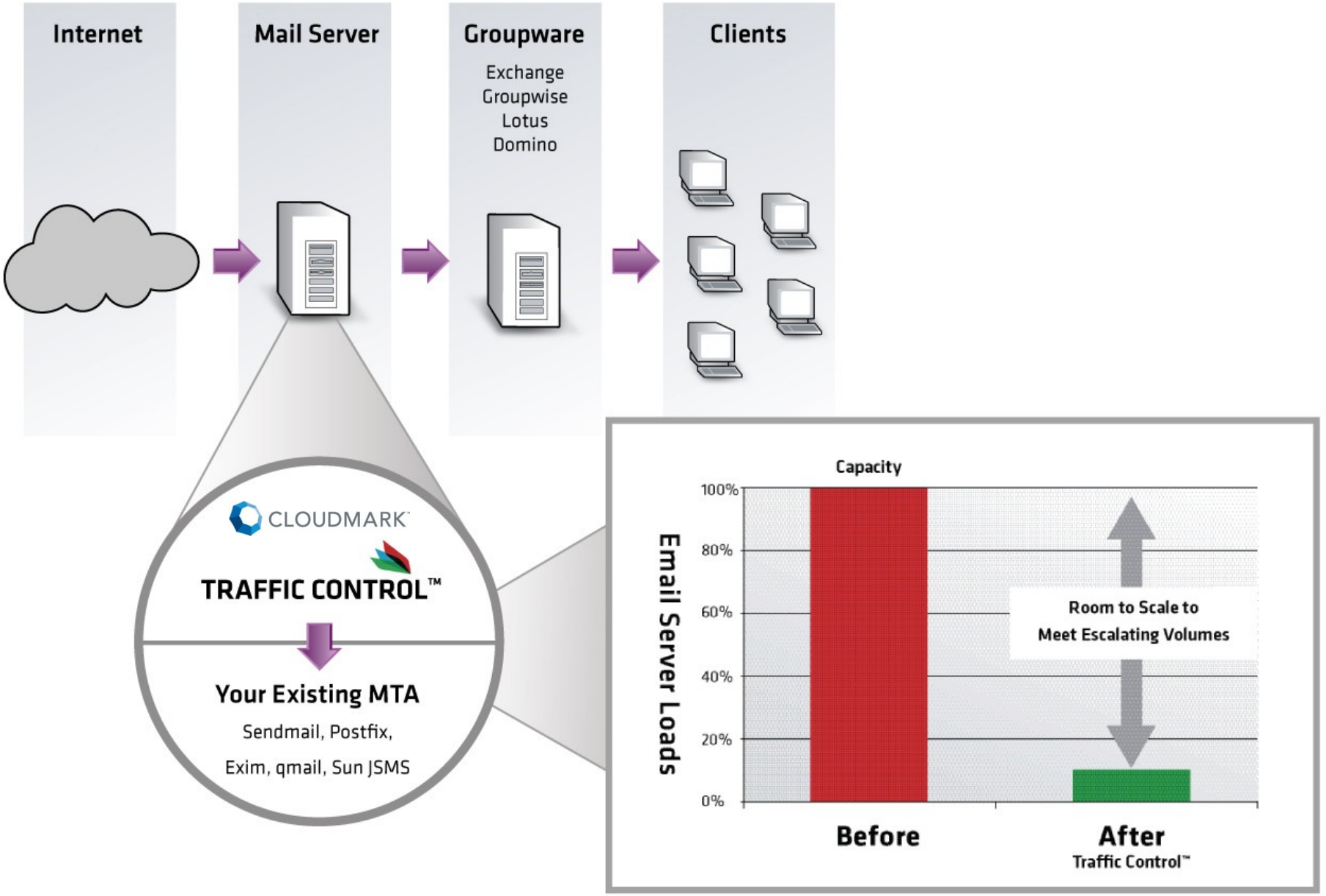
Six Overloaded Servers

October, 2006
After Traffic Control

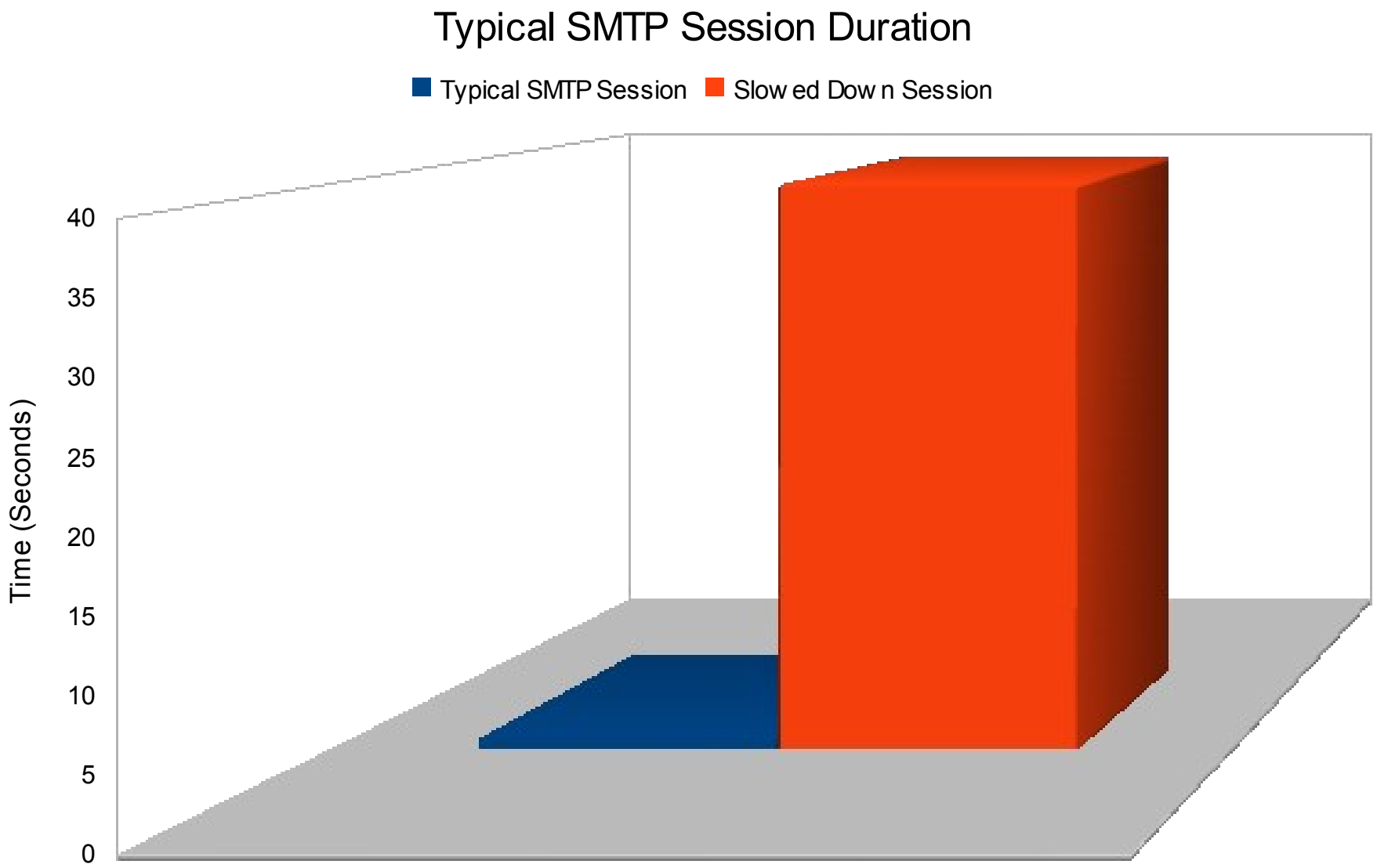


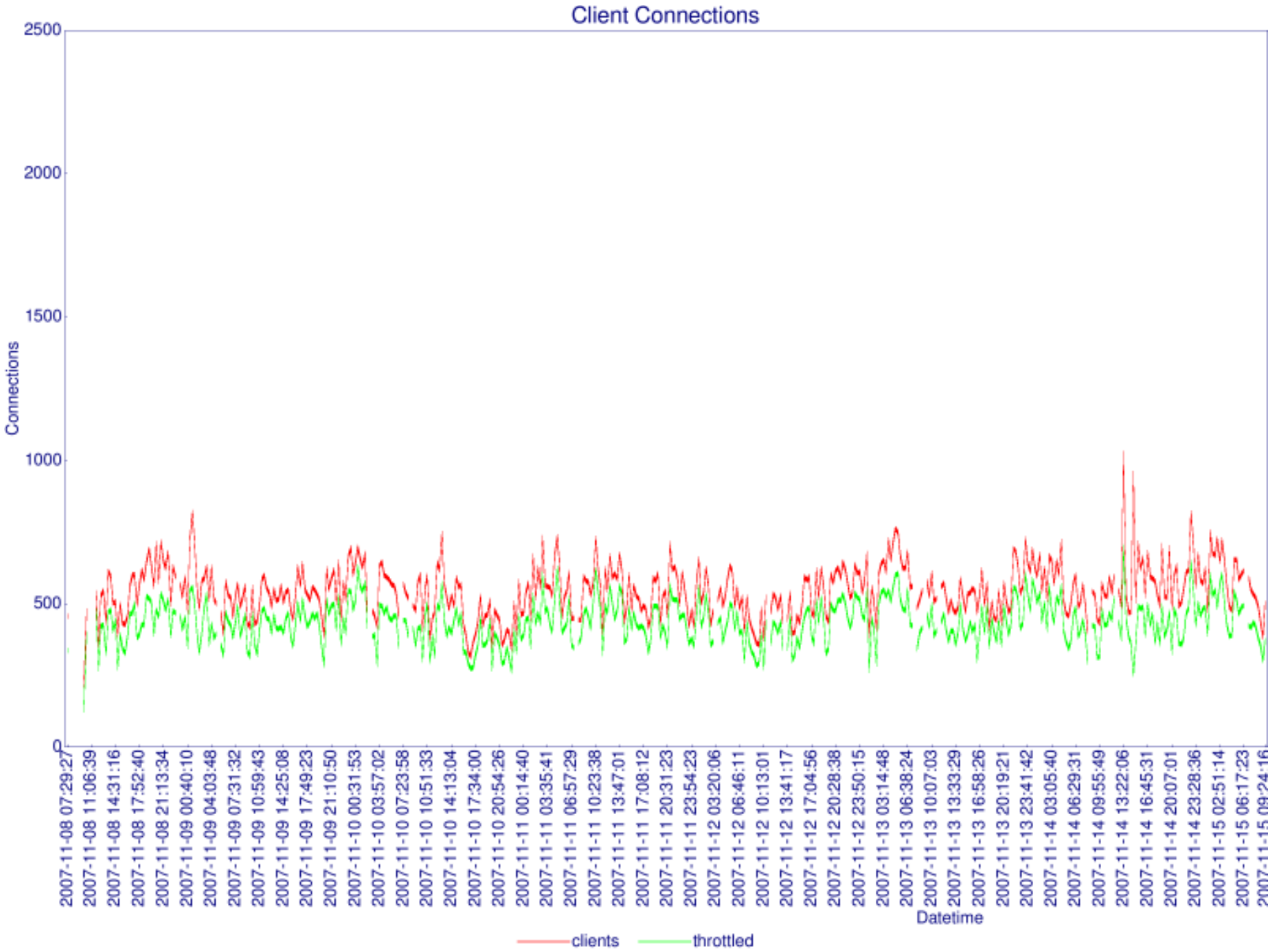
Two Servers


Millions
6
5
4
3
2
1
0
Total Messages
Spam
Traffic Control Installed
Jul-06
Aug-06
Sep-06
Oct-06
Nov-06
Dec-06
MAILCHANNELS

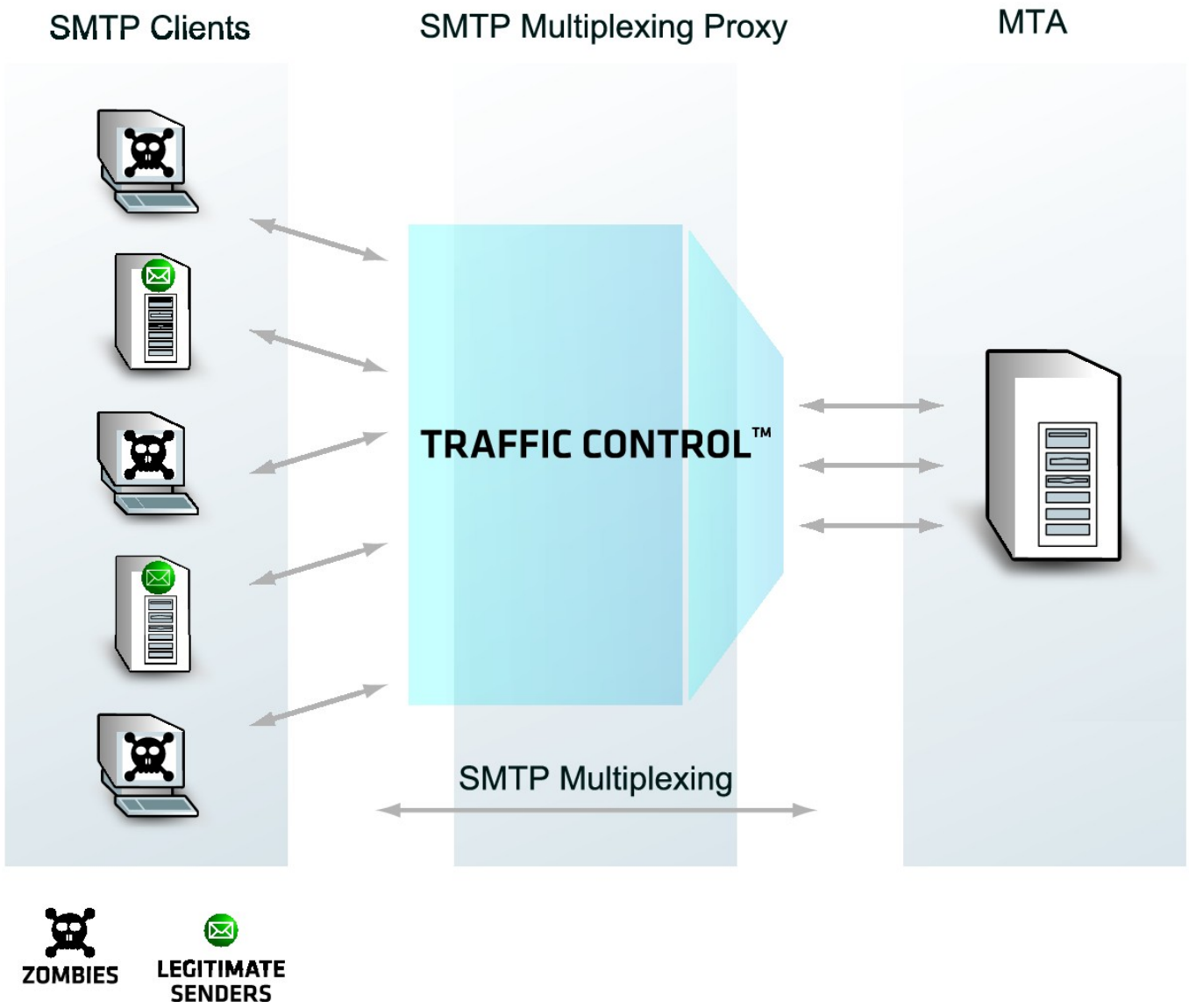

Internet
Mail Server
Groupware
Exchange
Groupwise
Lotus
Domino
Clients
CLOUDMARK
TRAFFIC CONTROL™
Your Existing MTA
Sendmail, Postfix,
Exim, qmail, Sun JSMS
Capacity
100%
80%
60%
40%
20%
0%
Email Server Loads
Room to Scale to
Meet Escalating Volumes
Before
After
Traffic Control™

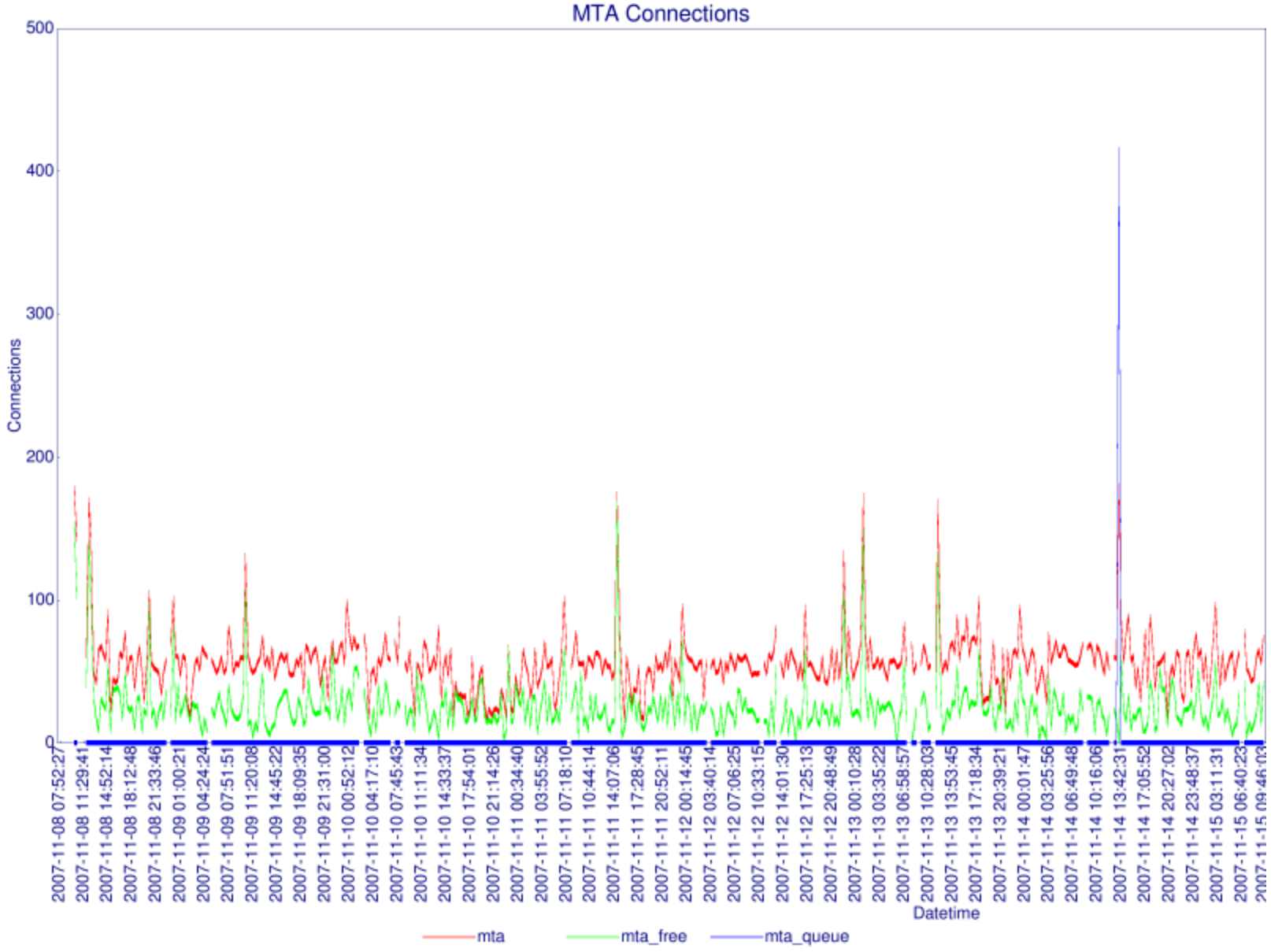

金鐘鳥
776-5459
心靈之約
Kt
DG-287


Typical SMTP Session Duration
Typical SMTP Session
Slowed Down Session
Time (Seconds)
40
35
30
25
20
15
10
5
0


Client Connections
2500
2000
1500
1000
500
0
Connections
2007-11-08 07:29:27
2007-11-08 11:06:39
2007-11-08 14:31:16
2007-11-08 17:52:40
2007-11-08 21:13:34
2007-11-09 00:40:10
2007-11-09 04:03:48
2007-11-09 07:31:32
2007-11-09 10:59:43
2007-11-09 14:25:08
2007-11-09 17:49:23
2007-11-09 21:10:50
2007-11-10 00:31:53
2007-11-10 03:57:02
2007-11-10 07:23:58
2007-11-10 10:51:33
2007-11-10 14:13:04
2007-11-10 17:34:00
2007-11-10 20:54:26
2007-11-11 00:14:40
2007-11-11 03:35:41
2007-11-11 06:57:29
2007-11-11 10:23:38
2007-11-11 13:47:01
2007-11-11 17:08:12
2007-11-11 20:31:23
2007-11-11 23:54:23
2007-11-12 03:20:06
2007-11-12 06:46:11
2007-11-12 10:13:01
2007-11-12 13:41:17
2007-11-12 17:04:56
2007-11-12 20:28:38
2007-11-12 23:50:15
2007-11-13 03:14:48
2007-11-13 06:38:24
2007-11-13 10:07:03
2007-11-13 13:33:29
2007-11-13 16:58:26
2007-11-13 20:19:21
2007-11-13 23:41:42
2007-11-14 03:05:40
2007-11-14 06:29:31
2007-11-14 09:55:49
2007-11-14 13:22:06
2007-11-14 16:45:31
2007-11-14 20:07:01
2007-11-14 23:28:36
2007-11-15 02:51:14
2007-11-15 06:17:23
2007-11-15 09:24:16
Datetime
clients
throttled

Traffic Control: Second Generation: SMTP Proxy Internals

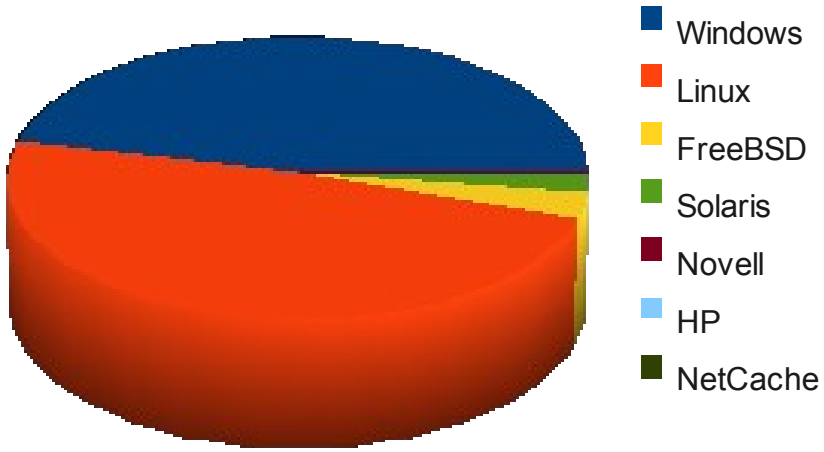



MTA Connections
Connections
500
400
300
200
100
0
2007-11-08 07:52:27
2007-11-08 11:29:41
2007-11-08 14:52:14
2007-11-08 18:12:48
2007-11-08 21:33:46
2007-11-09 01:00:21
2007-11-09 04:24:24
2007-11-09 07:51:51
2007-11-09 11:20:08
2007-11-09 14:45:22
2007-11-09 18:09:35
2007-11-09 21:31:00
2007-11-10 00:52:12
2007-11-10 04:17:10
2007-11-10 07:45:43
2007-11-10 11:11:34
2007-11-10 14:33:37
2007-11-10 17:54:01
2007-11-10 21:14:26
2007-11-11 00:34:40
2007-11-11 03:55:52
2007-11-11 07:18:10
2007-11-11 10:44:14
2007-11-11 14:07:06
2007-11-11 17:28:45
2007-11-11 20:52:11
2007-11-12 00:14:45
2007-11-12 03:40:14
2007-11-12 07:06:25
2007-11-12 10:33:15
2007-11-12 14:01:30
2007-11-12 17:25:13
2007-11-12 20:48:49
2007-11-13 00:10:28
2007-11-13 03:35:22
2007-11-13 06:58:57
2007-11-13 10:28:03
2007-11-13 13:53:45
2007-11-13 17:18:34
2007-11-13 20:39:21
2007-11-14 00:01:47
2007-11-14 03:25:56
2007-11-14 06:49:48
2007-11-14 10:16:06
2007-11-14 13:42:31
2007-11-14 17:05:52
2007-11-14 20:27:02
2007-11-14 23:48:37
2007-11-15 03:11:31
2007-11-15 06:40:23
2007-11-15 09:46:03
Datetime
mta
mta_free
mta_queue

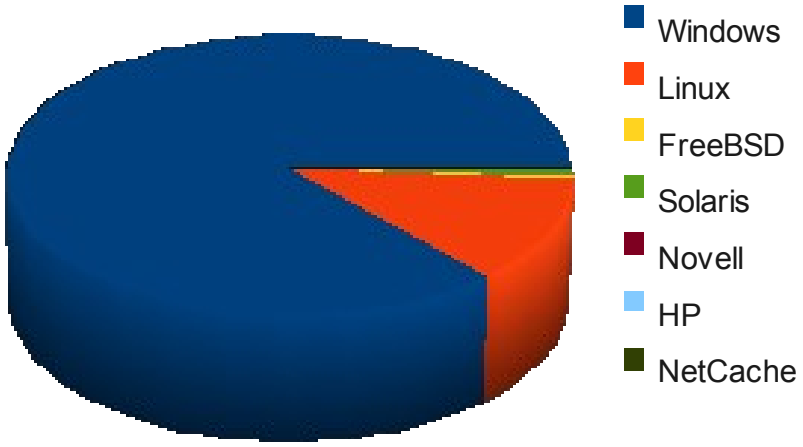
MAILCHANNELS

One of these kids is not like the others...

Delivered



Not delivered



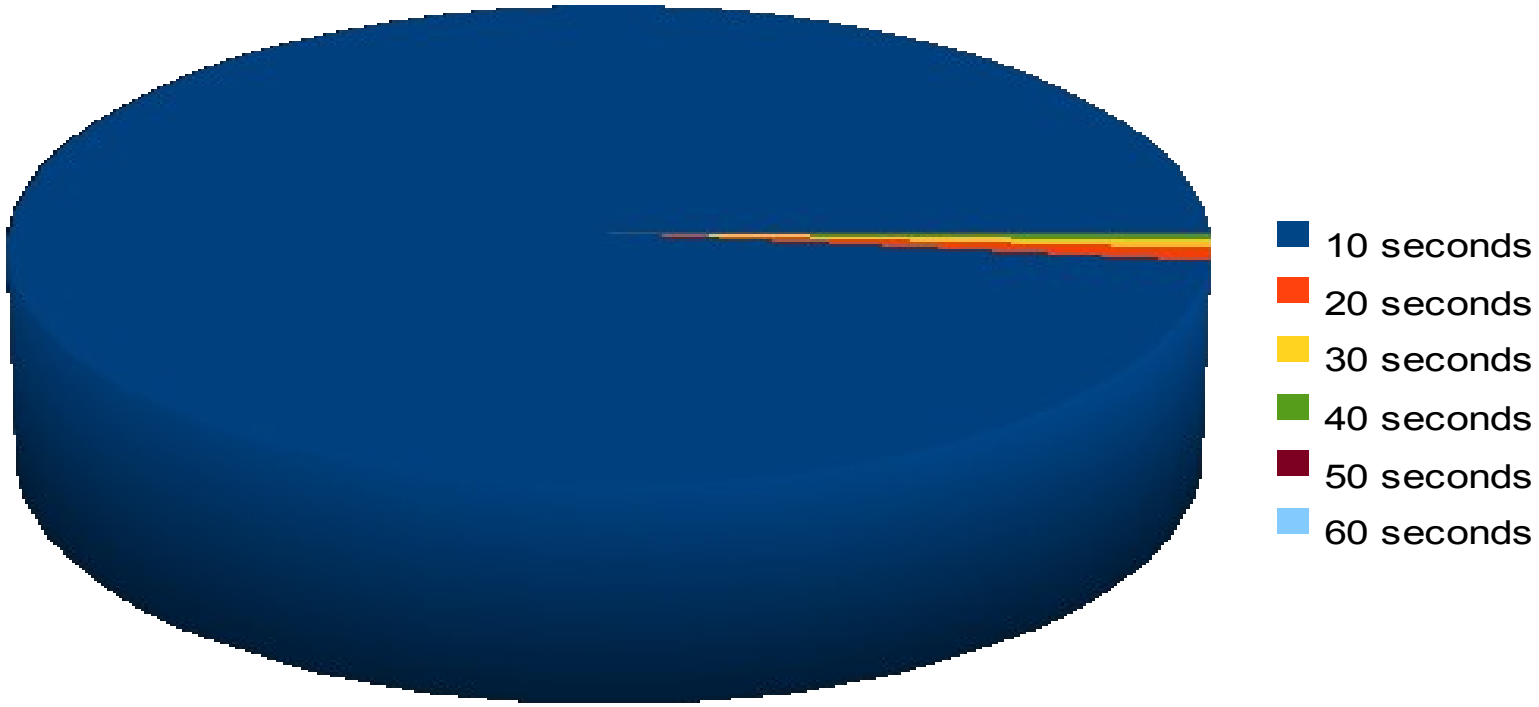
MAILCHANNELS

Storm Botnet Throttling

- RBLs rejected 70% of the likely Storm botnet zombies
- Of those that remained...
  - 74% did not complete delivery of a message
    - 10% were detected as consumer operating systems (Windows 98, Windows XP, etc.)
    - The rest were unknown, and therefore throttled

MAILCHANNELS

A Passing Storm



MAILCHANNELS

Conclusions

1. Spamming is driven by economics
2. Botnet operators need to make money
3. Slowing down spam makes it go away

- Beer & Spam at 8:30pm
  Room: “Reunion G”

Nick Shelness, Former CTO, Lotus:

“I am able to report that I have been running an instance of TrafficControl in my own network for four months, and that it has reduced the volume of spam hitting my boundary MTAs on most days by approximately 95%.”

questions@mailchannels.com

+1-778-785-6143

www.mailchannels.com