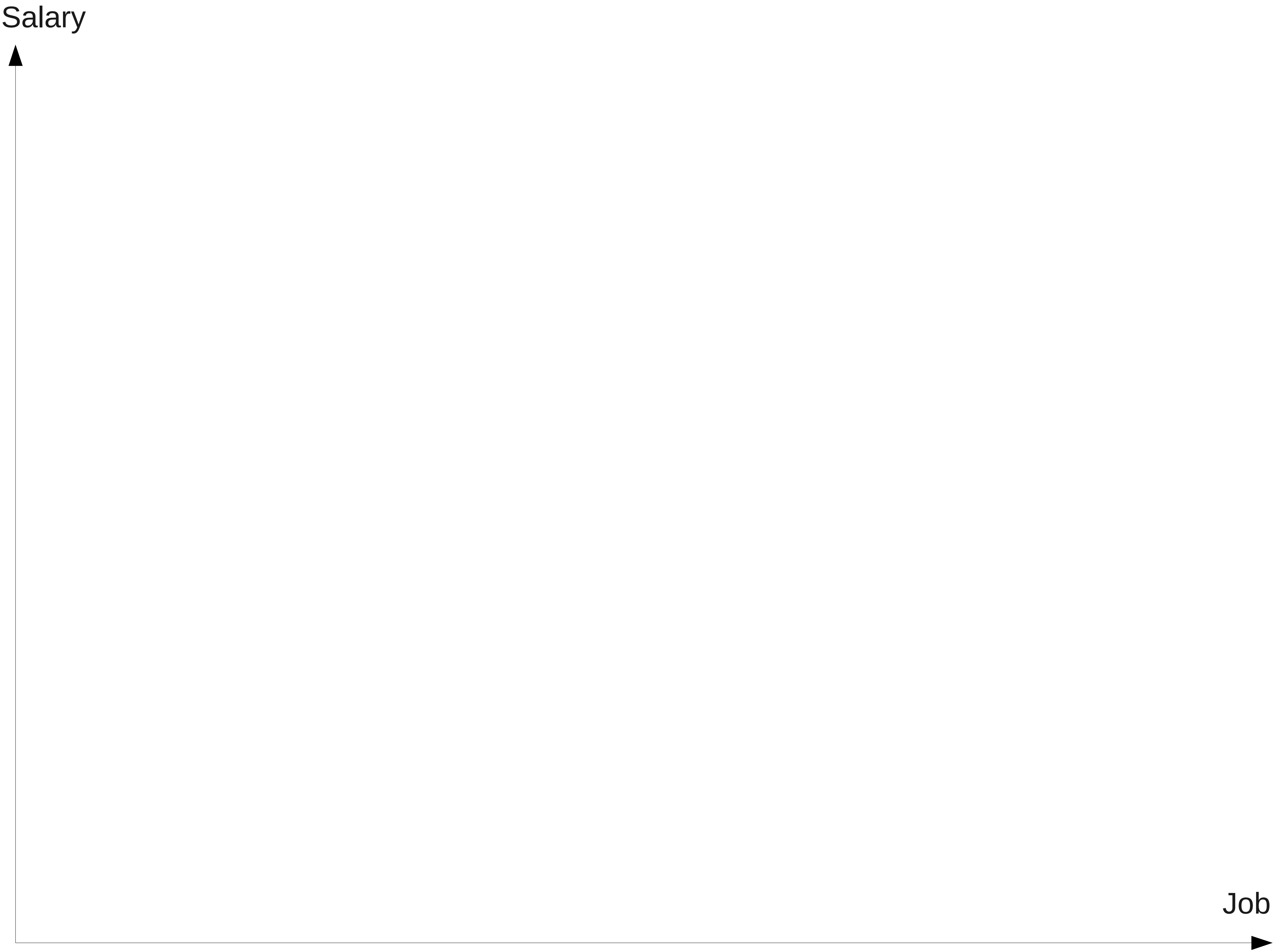
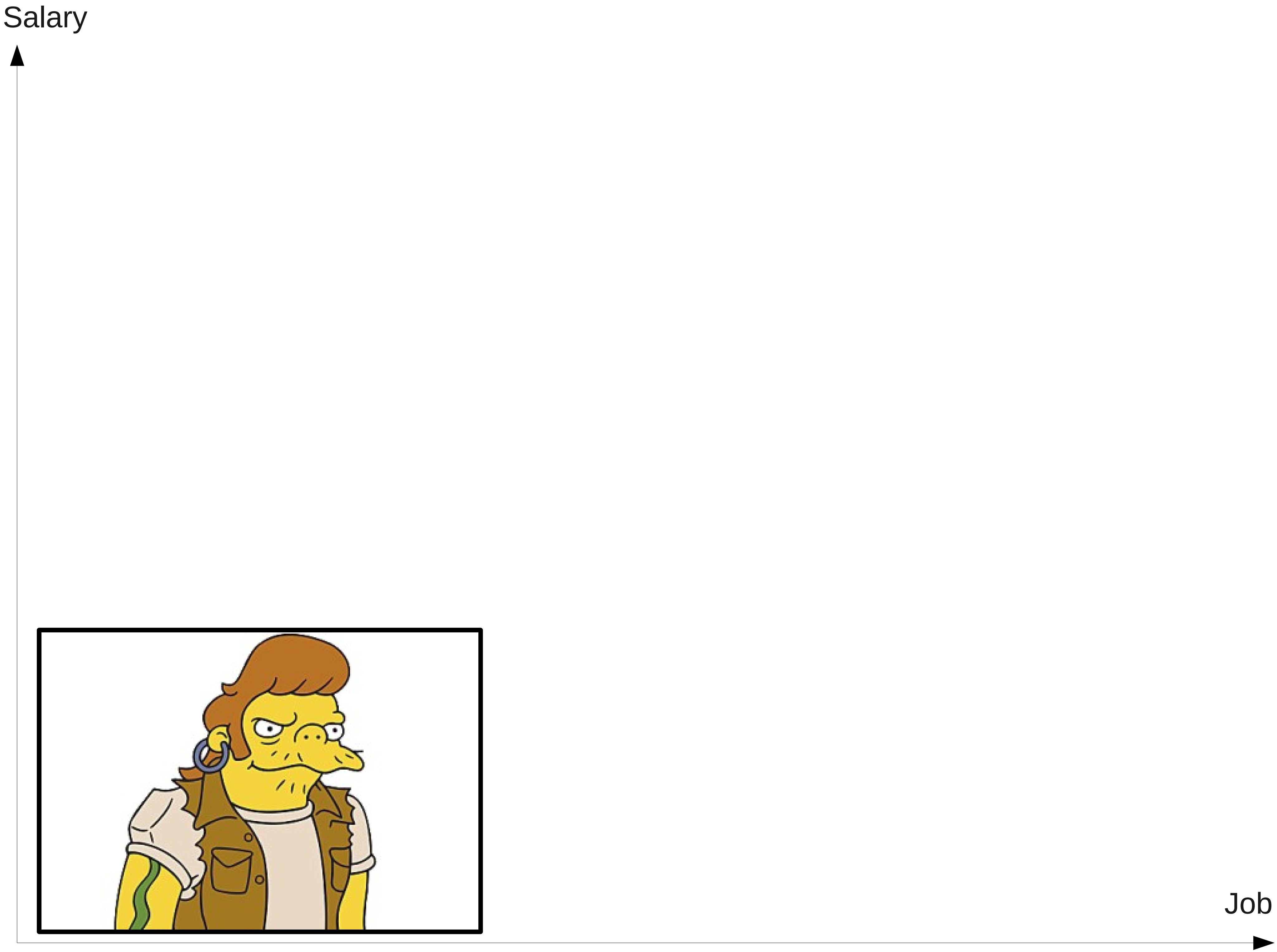
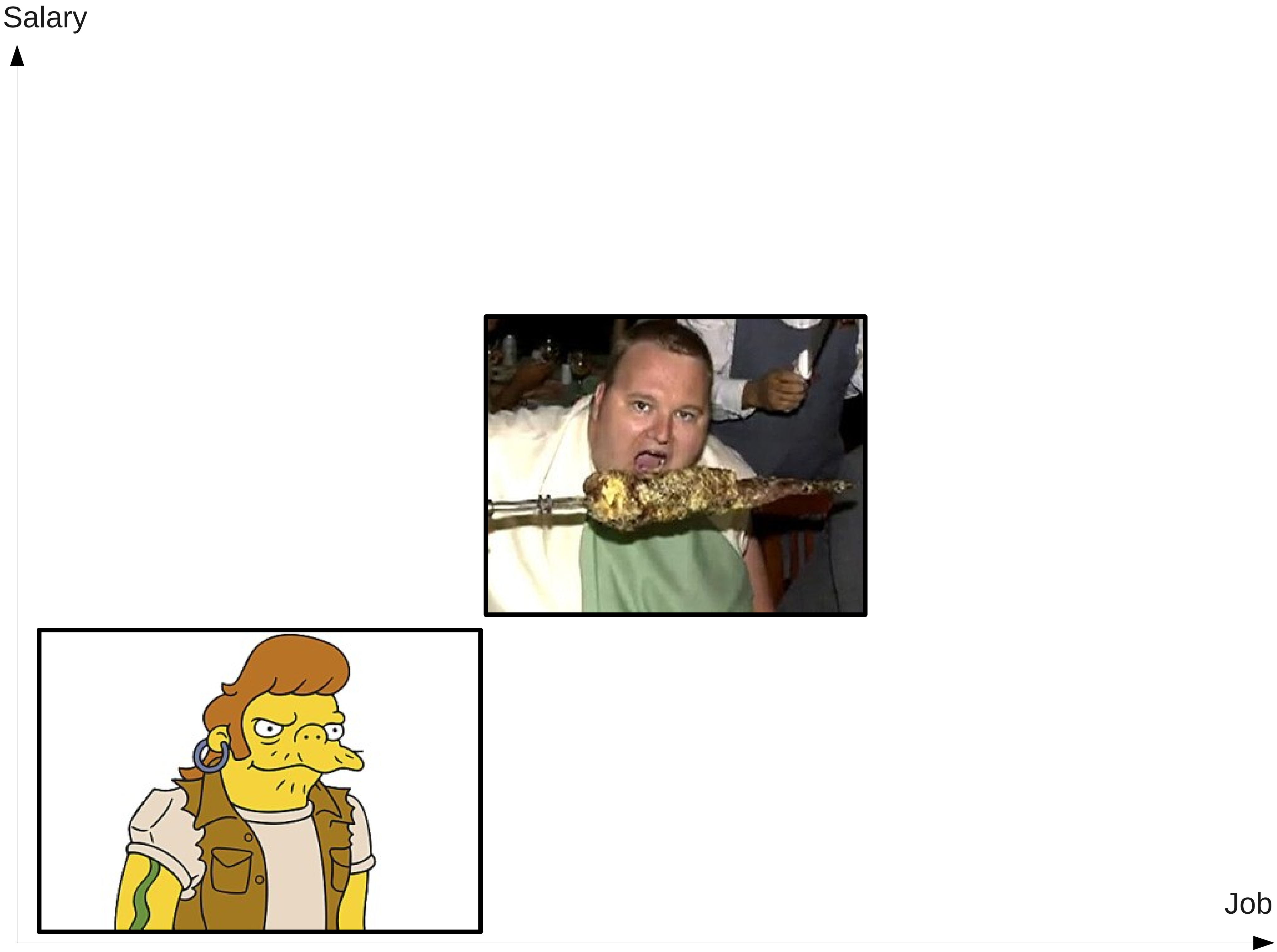
Lose weight Limited time only Save big money **Viagra** Supplies are limited Take action now No disappointment Nitroglycerin **Dear friend** No questions asked Offer expires Work at home You have been selected McCain Says Unsure If Obama A Secret Hippopotamus Urgent Unlimited This isn’t spam Social security number Serious cash Free membership Click to remove mailto Outstanding values Online pharmacy Act now! Don’t hesitate! Potential earnings Contemporary Spam Fighting Reverses aging Lowest price Meet singles Sign up free today Opportunity **Risk free** Removes wrinkles Financial freedom Full refund Christoph Niemz No strings attached What are you waiting for? No medical exams Once in lifetime ETH Zürich Extra cash passwords Free cell phone **Fast Viagra delivery** Drastically reduced Don’t delete Congratulations Click here link Avoid bankruptcy Additional income **Great offer** Accept credit cards 07.03.2012 Join millions of Americans

Lose weight Limited time only Save big money **Viagra** Supplies are limited Take action now No disappointment Nitroglycerin **Dear friend** No questions asked Offer expires Work at home You have been selected McCain Says Unsure If Obama A Secret Hippopotamus Urgent Unlimited This isn't spam Social security number Serious cash Free membership Click to remove mailto Outstanding values Online pharmacy Act now! Don't hesitate! Potential earnings **Contemporary Spam Fighting** Reverses aging Lowest price Meet singles Sign up free today Opportunity **Risk free** Removes wrinkles Financial freedom Full refund **Christoph Niemz** No strings attached What are you waiting for? No medical exams Once in lifetime **ETH Zürich** Extra cash passwords Free cell phone **Fast Viagra delivery** Drastically reduced Don't delete Congratulations Click here link Avoid bankruptcy Additional income **Great offer** Accept credit cards **07.03.2012** Join millions of Americans


Salary
Job


Salary
Job



Salary

Job

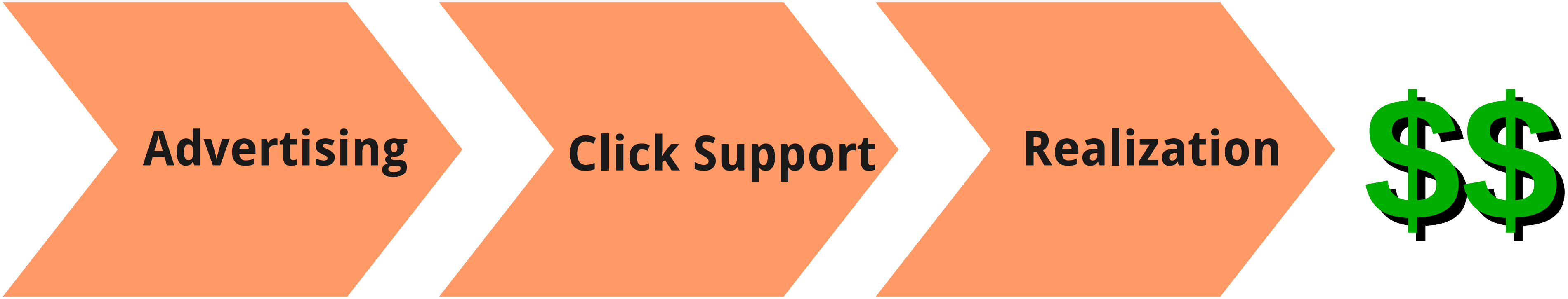
Salary
Job

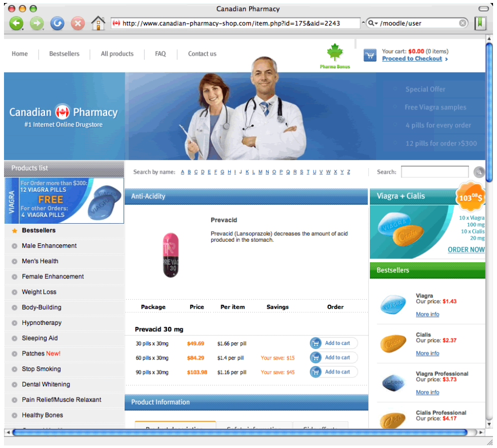
Salary
Job
SPAM

Outline

$$

The Value Chain of Spam





Your cart: $0.00 (0 items)
Proceed to Checkout ›

For Order more than $300:
12 VIAGRA PILLS
FREE
For other Orders:
4 VIAGRA PILLS

Prevacid

Prevacid (Lansoprazole) decreases the amount of acid produced in the stomach.

Package	Price	Per item	Savings	Order
Prevacid 30 mg				
30 pills x 30mg	$49.69	$1.66 per pill		Add to cart
60 pills x 30mg	$84.29	$1.4 per pill	Your save: $15	Add to cart
90 pills x 30mg	$103.98	$1.16 per pill	Your save: $45	Add to cart

10 x Viagra 100 mg
10 x Cialis 20 mg

Viagra
Our price: $1.43
More info

Cialis
Our price: $2.37
More info

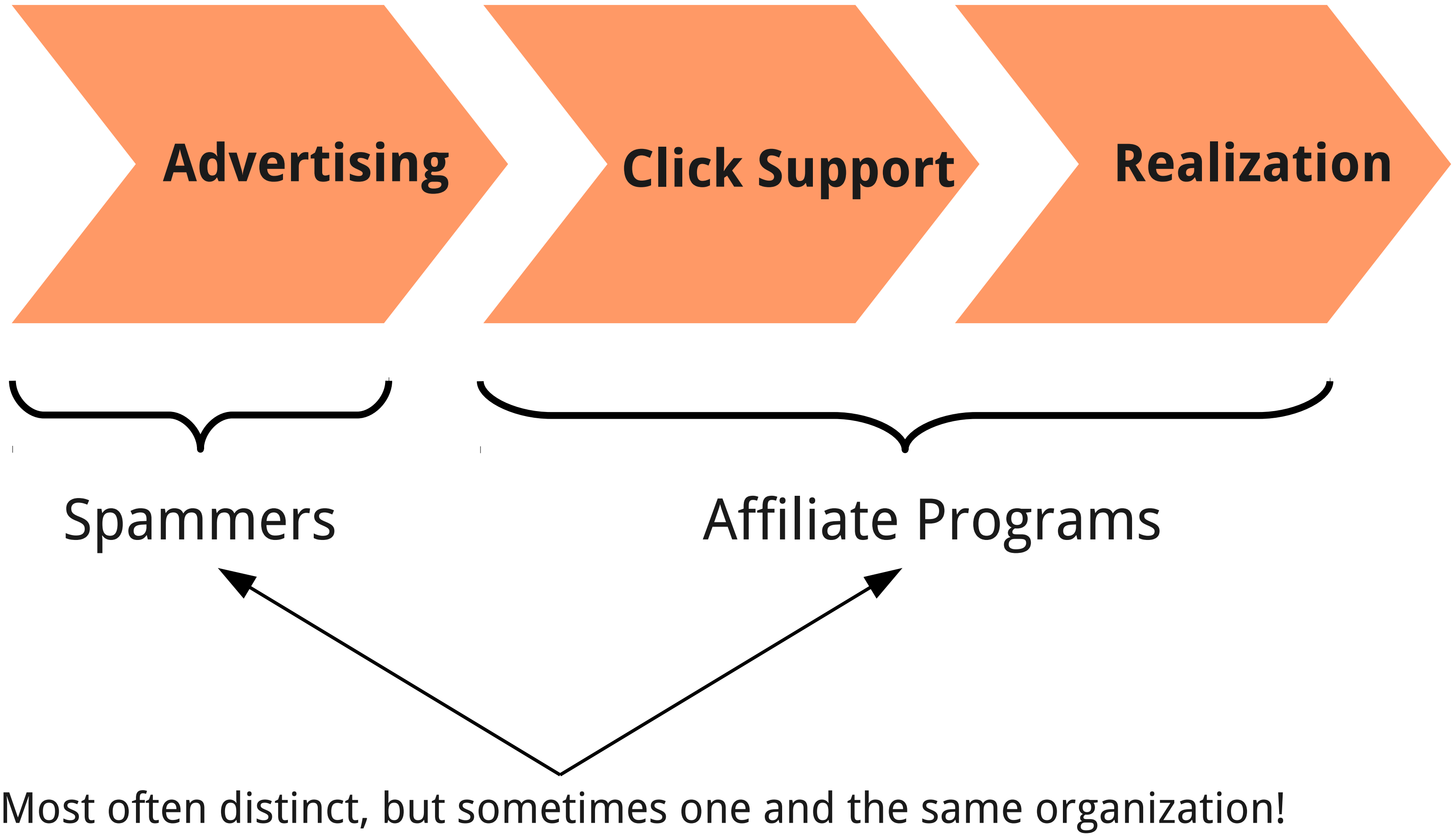
Viagra Professional
Our price: $3.73
More info

Cialis Professional
Our price: $4.17

VISA

MasterCard

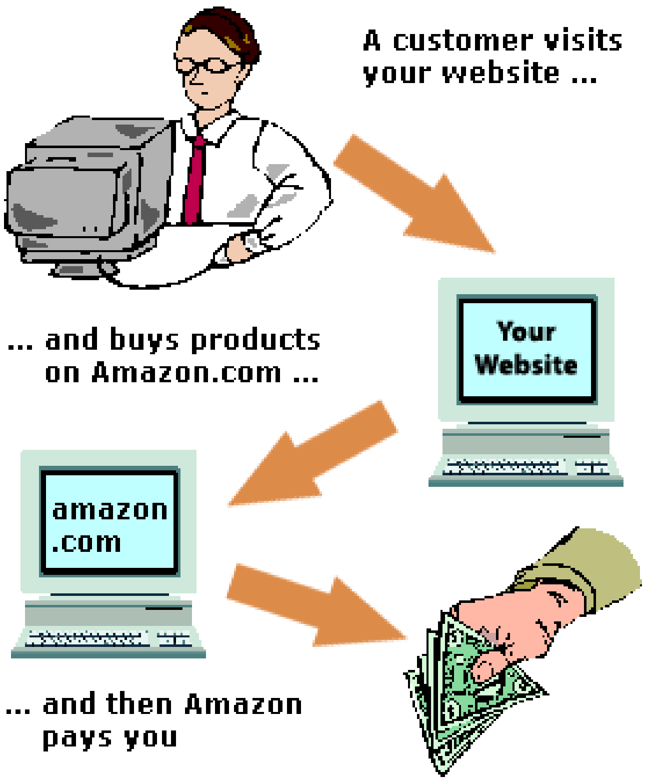
Actors in the Spam Value Chain



Most often distinct, but sometimes one and the same organization!

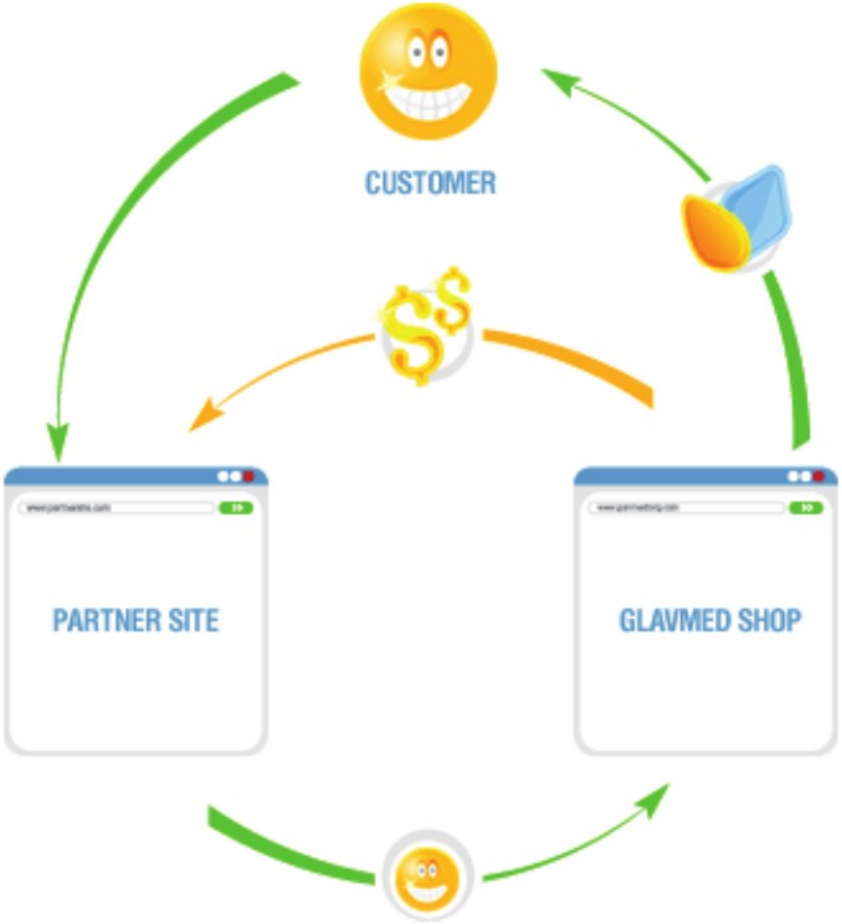
Affiliate Programs

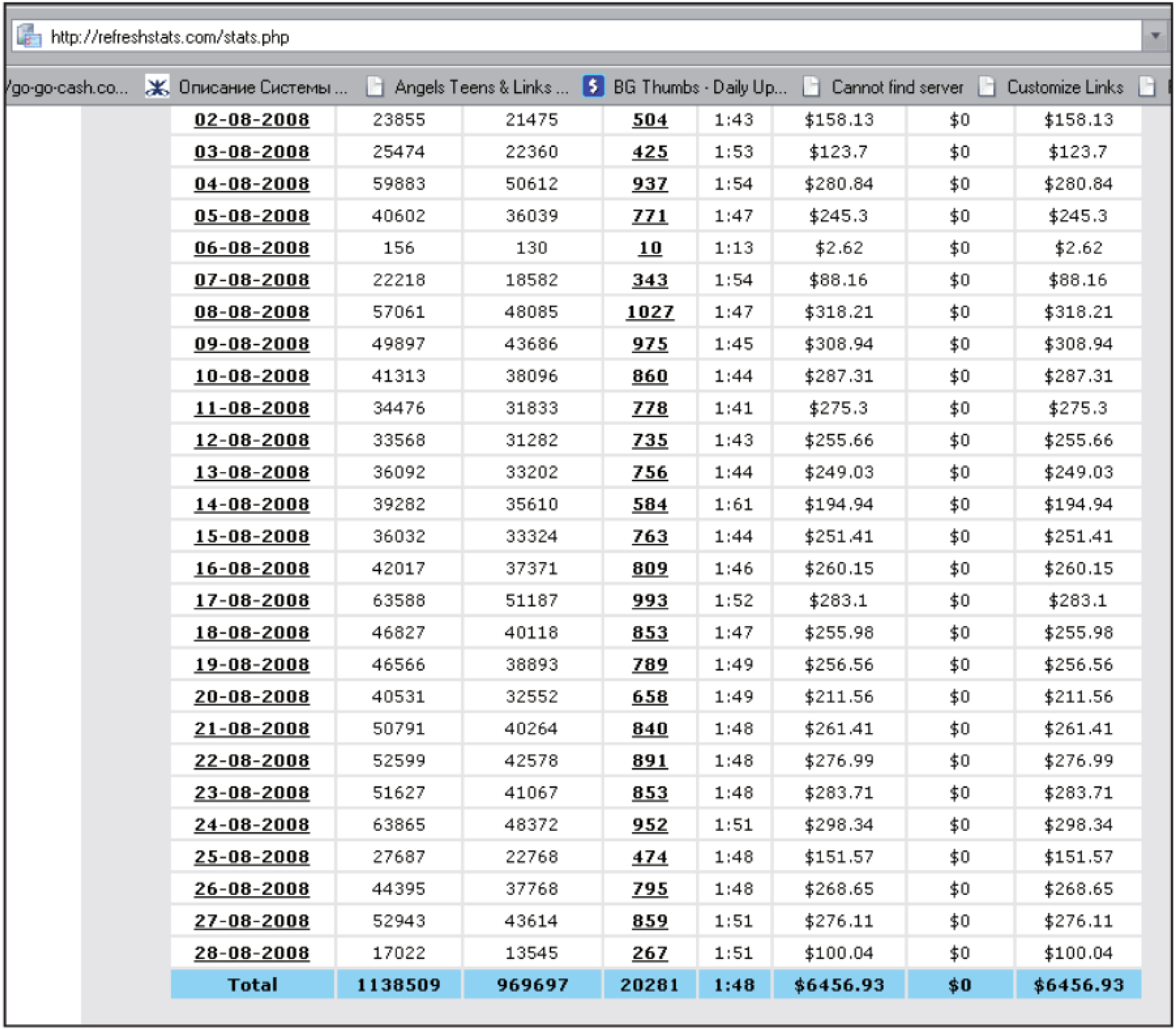
For each successful sale, you get a commission of 4-15% from Amazon



Affiliate Programs

For each successful sale, the spammer gets a commission of 30-50% from e.g. GlavMed





02-08-2008	23855	21475	504	1:43	$158.13	$0	$158.13
03-08-2008	25474	22360	425	1:53	$123.7	$0	$123.7
04-08-2008	59883	50612	937	1:54	$280.84	$0	$280.84
05-08-2008	40602	36039	771	1:47	$245.3	$0	$245.3
06-08-2008	156	130	10	1:13	$2.62	$0	$2.62
07-08-2008	22218	18582	343	1:54	$88.16	$0	$88.16
08-08-2008	57061	48085	1027	1:47	$318.21	$0	$318.21
09-08-2008	49897	43686	975	1:45	$308.94	$0	$308.94
10-08-2008	41313	38096	860	1:44	$287.31	$0	$287.31
11-08-2008	34476	31833	778	1:41	$275.3	$0	$275.3
12-08-2008	33568	31282	735	1:43	$255.66	$0	$255.66
13-08-2008	36092	33202	756	1:44	$249.03	$0	$249.03
14-08-2008	39282	35610	584	1:61	$194.94	$0	$194.94
15-08-2008	36032	33324	763	1:44	$251.41	$0	$251.41
16-08-2008	42017	37371	809	1:46	$260.15	$0	$260.15
17-08-2008	63588	51187	993	1:52	$283.1	$0	$283.1
18-08-2008	46827	40118	853	1:47	$255.98	$0	$255.98
19-08-2008	46566	38893	789	1:49	$256.56	$0	$256.56
20-08-2008	40531	32552	658	1:49	$211.56	$0	$211.56
21-08-2008	50791	40264	840	1:48	$261.41	$0	$261.41
22-08-2008	52599	42578	891	1:48	$276.99	$0	$276.99
23-08-2008	51627	41067	853	1:48	$283.71	$0	$283.71
24-08-2008	63865	48372	952	1:51	$298.34	$0	$298.34
25-08-2008	27687	22768	474	1:48	$151.57	$0	$151.57
26-08-2008	44395	37768	795	1:48	$268.65	$0	$268.65
27-08-2008	52943	43614	859	1:51	$276.11	$0	$276.11
28-08-2008	17022	13545	267	1:51	$100.04	$0	$100.04
Total	**1138509**	**969697**	**20281**	**1:48**	**$6456.93**	**$0**	**$6456.93**

Source: The Partnerka – What is it, and why should you care?

Conversion Rate Analysis [Storm Botnet]

0.0000081% of all emails sent lead to a customer buying a spam-advertised pharma product.

⇔

Spammer needs to send ≈ 12 500 000 mails until one customer places an order!

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Conversion Rate Analysis [Storm Botnet]

With an average order price of $100,
the Storm Botnet ”produced” revenues of ≈
$9500/day ⇔ $3.5 mio./year

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Is Spamming Profitable? [Storm Botnet]

+ $3.5 mio. Annual Revenue

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Is Spamming Profitable? [Storm Botnet]

+ $3.5 mio.	Annual Revenue
- $1.75 mio.	50% for Affiliate Program

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Is Spamming Profitable? [Storm Botnet]

+ $3.5 mio.	Annual Revenue
- $1.75 mio.	50% for Affiliate Program
- $26 mio.	(≈ $80 for domain names & bulletproof hosting for 1 mio. mails) x 328 000 mio. mails sent

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Is Spamming Profitable? [Storm Botnet]

+ $3.5 mio.	Annual Revenue
- $1.75 mio.	50% for Affiliate Program
- $26 mio.	(≈ $80 for domain names & bulletproof hosting for 1 mio. mails) x 328 000 mio. mails sent
- $24.25 mio.	

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Is Spamming Profitable? [Storm Botnet]

+ $3.5 mio.	Annual Revenue
- $1.75 mio.	50% for Affiliate Program
- $26 mio.	(≈ $80 for domain names & bulletproof hosting for 1 mio. mails) x 328 000 mio. mails sent

- $24.25 mio.

The Storm operators probably
do everything ”under one roof”

Source: Spamalytics: An Empirical Analysis of Spam Marketing Conversion

The Economic Damage of Spam

- Estimated cost for deleting spam by hand in the US ≈ $22 bio. / year

- Other Cost Factors:
  - Mail Filters
  - Additional IT Infrastructure
  - Loss of Network Bandwidth

Source: http://technoreadymarketing.com/Articles/Summary%20Report-NTRS%202004.pdf

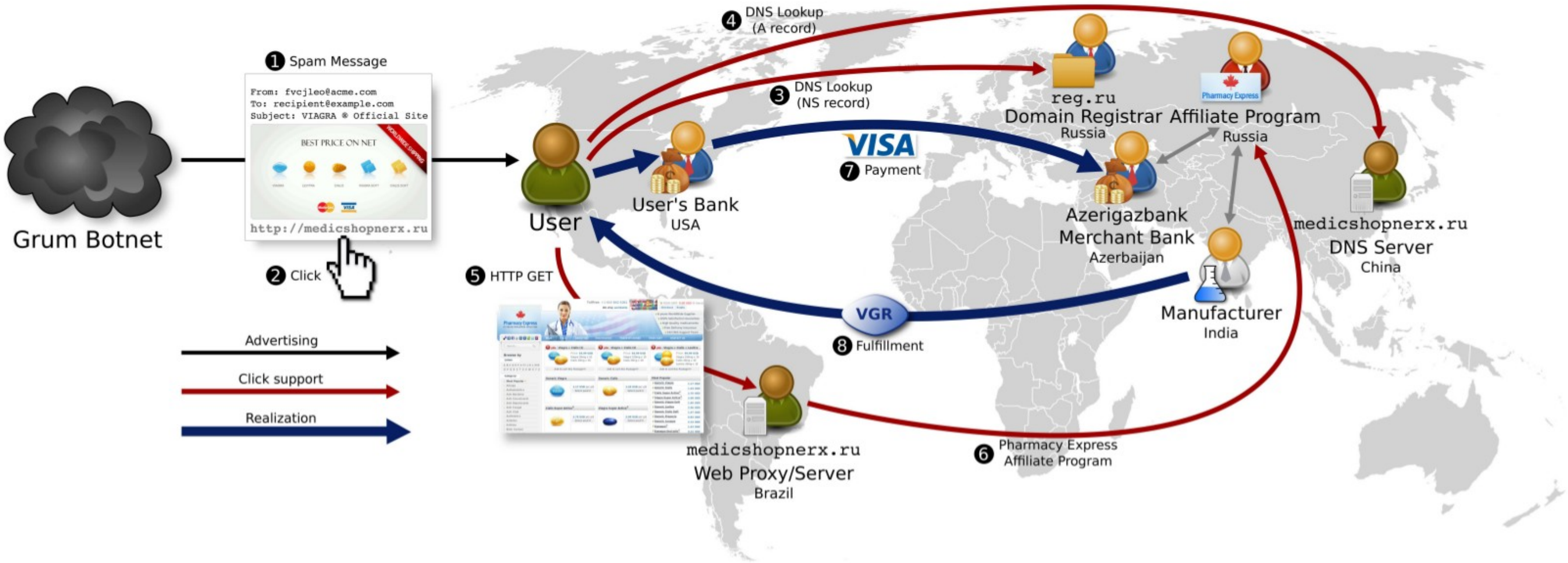
Curious Facts

- ≈ 4-7% of people who read a spam mail buy products advertised by this mail
- ≈ 88% settled orders were actually delivered to the customer!
- ≈ 20% of the customers come back!

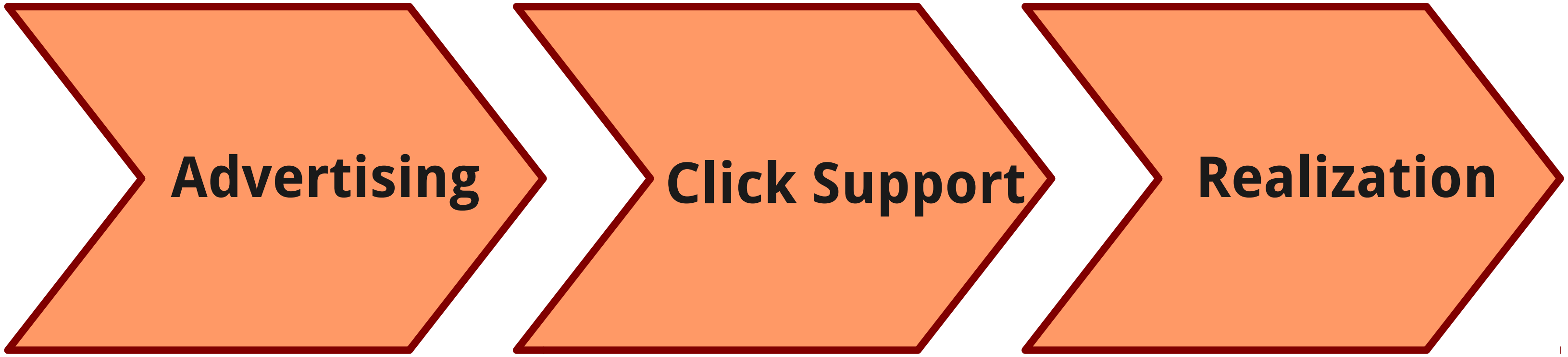
Sources: http://technoreadymarketing.com/Articles/Summary%20Report-NTRS%202004.pdf
Click-Trajectories: End-to-End Analysis of the Spam Value Chain

So let's just shutdown their servers!

Why it's not that easy...



Bottleneck Analysis of the Spam Value Chain

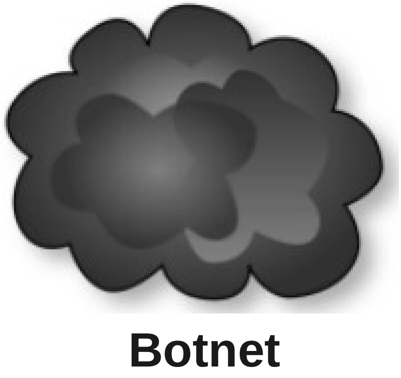


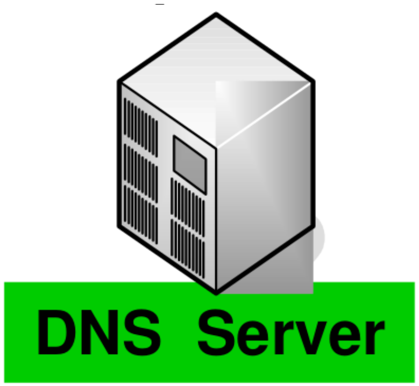
Advertising

Click Support

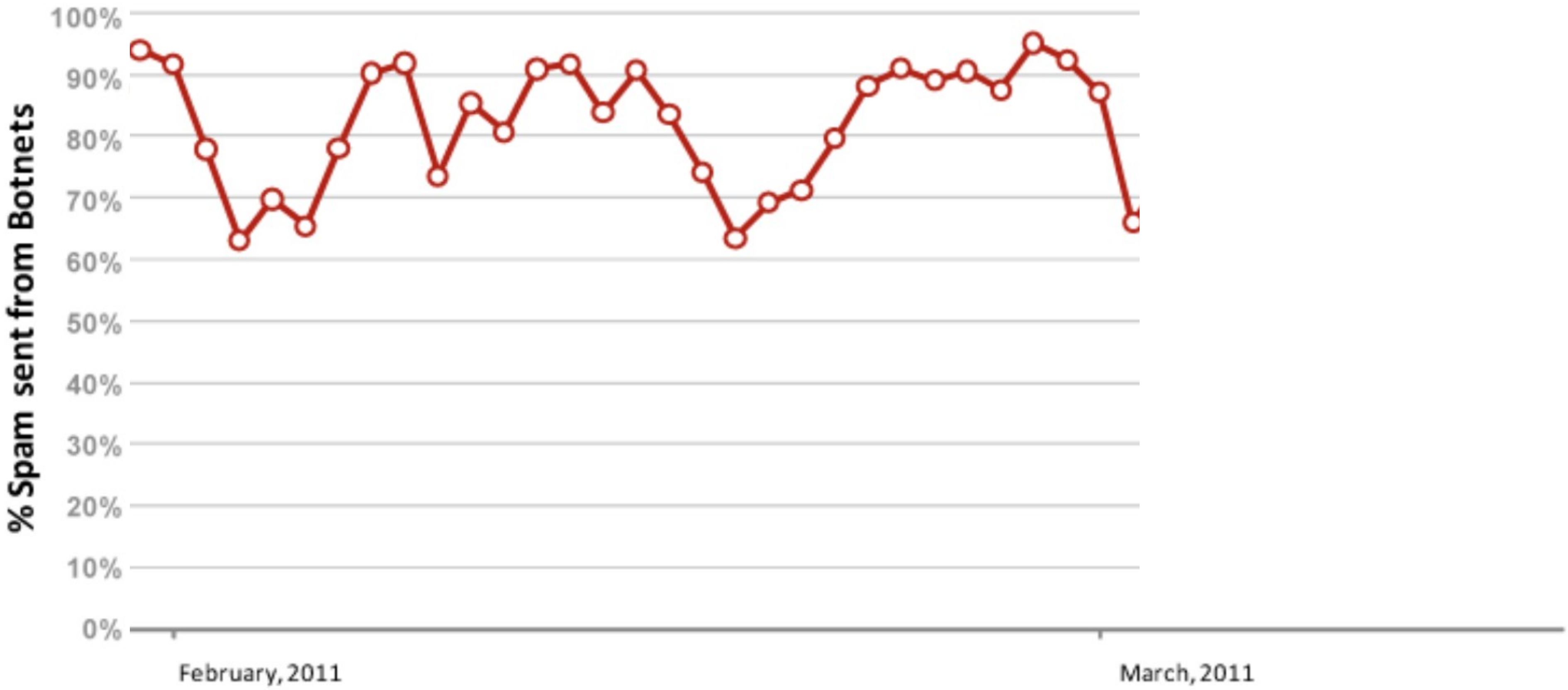
Realization

Potential Bottlenecks



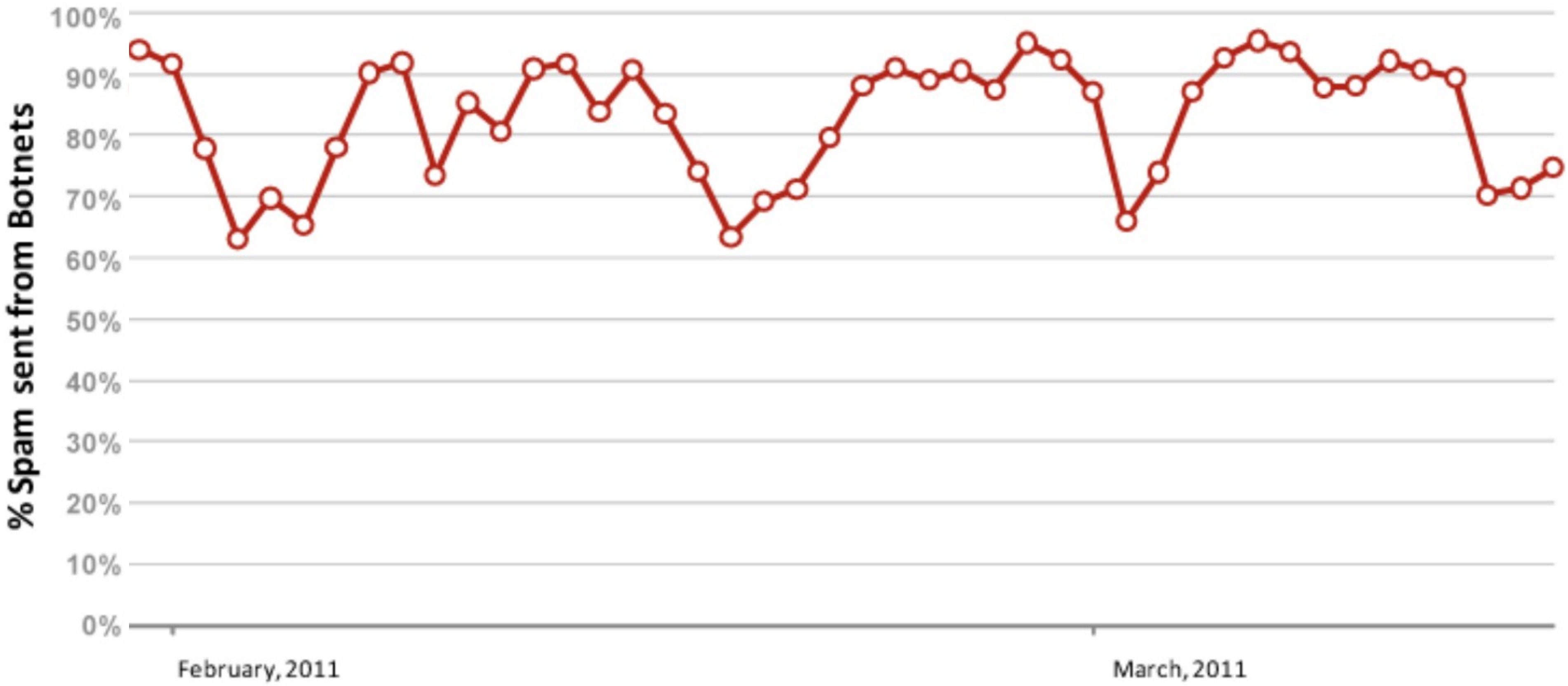


Botnet Takedown Effectiveness



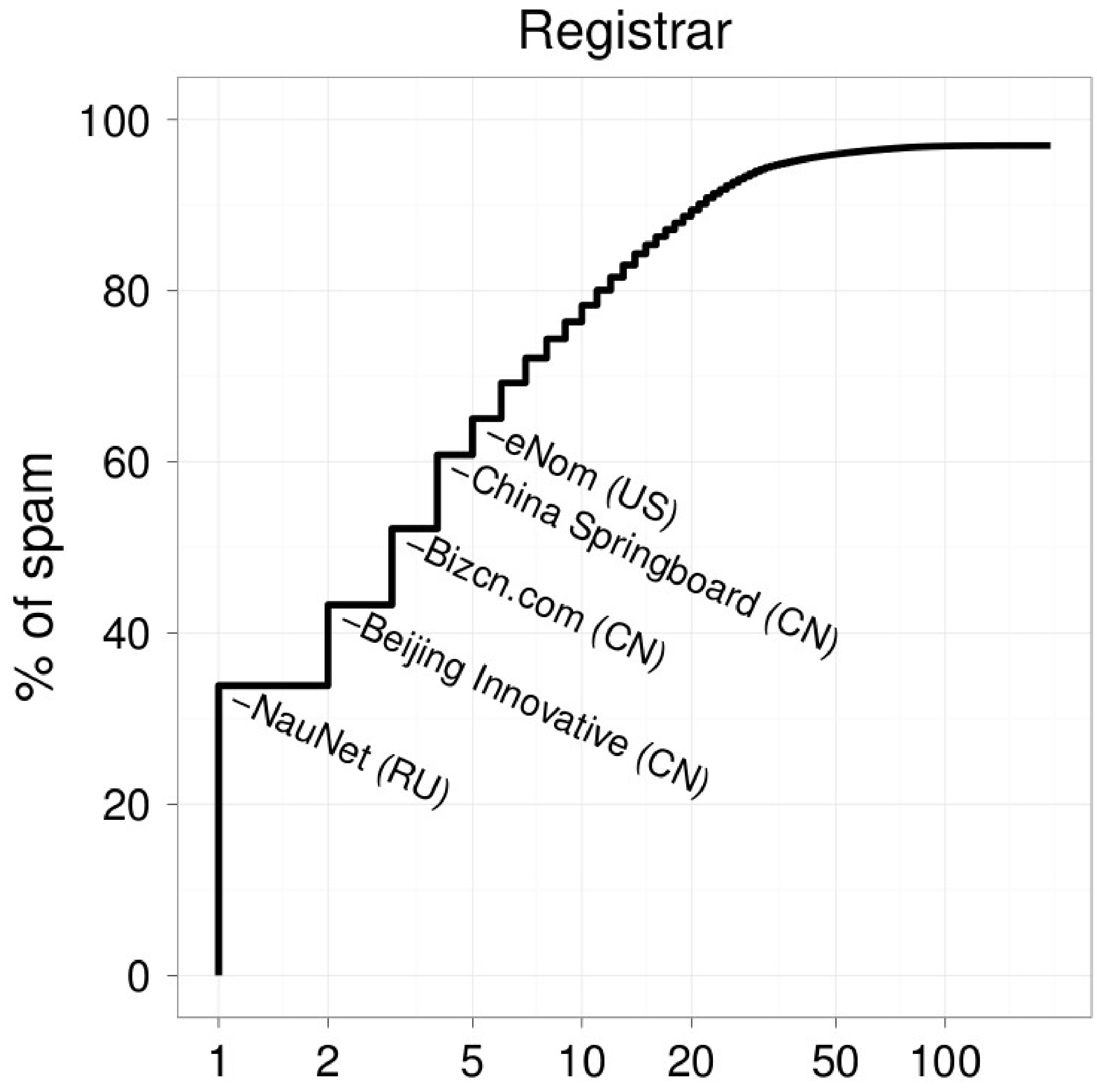
Source: MessageLab March 2011 Intelligence Report

Botnet Takedown Effectiveness



Source: MessageLab March 2011 Intelligence Report

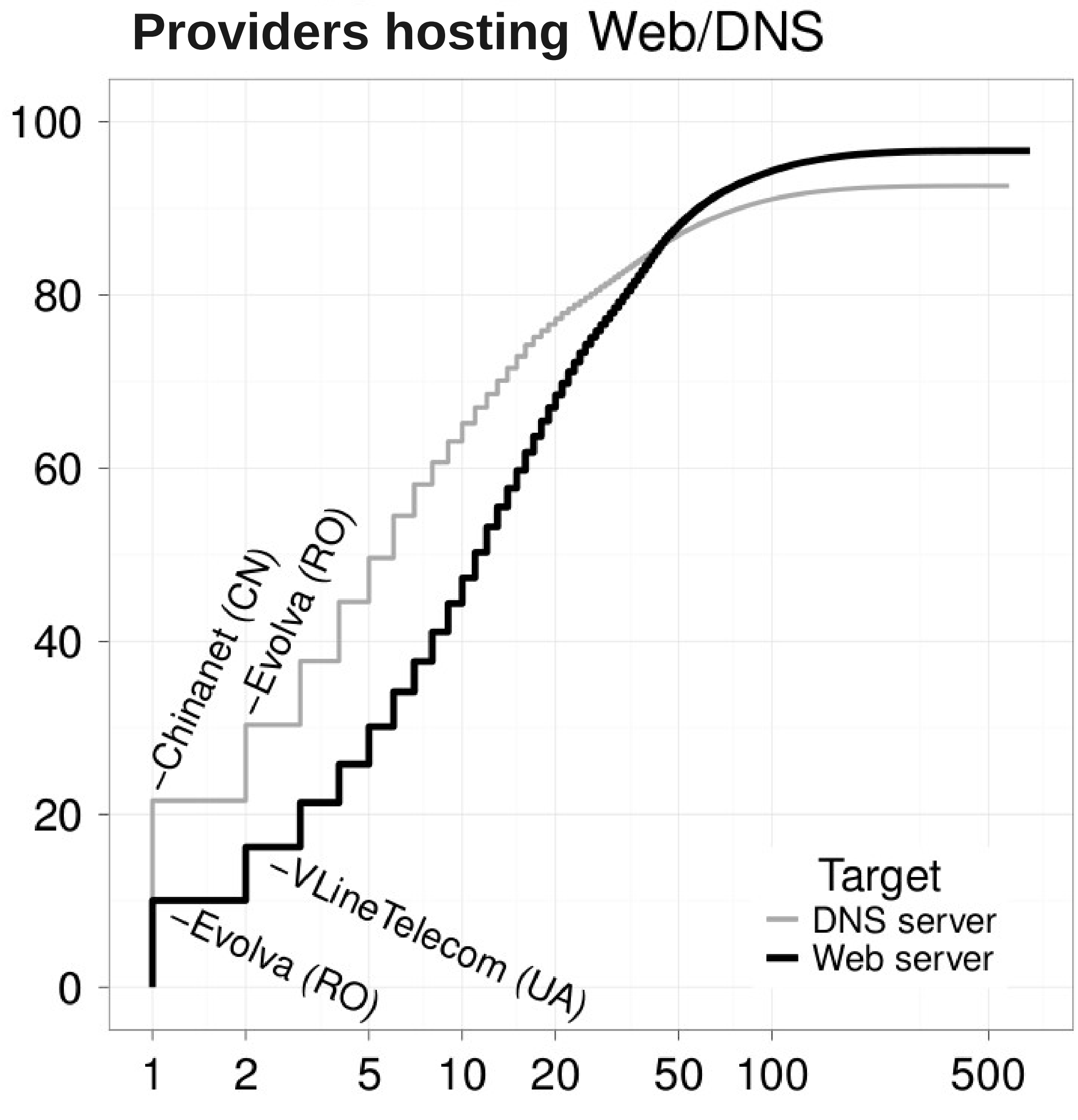
Domain Name Registrars



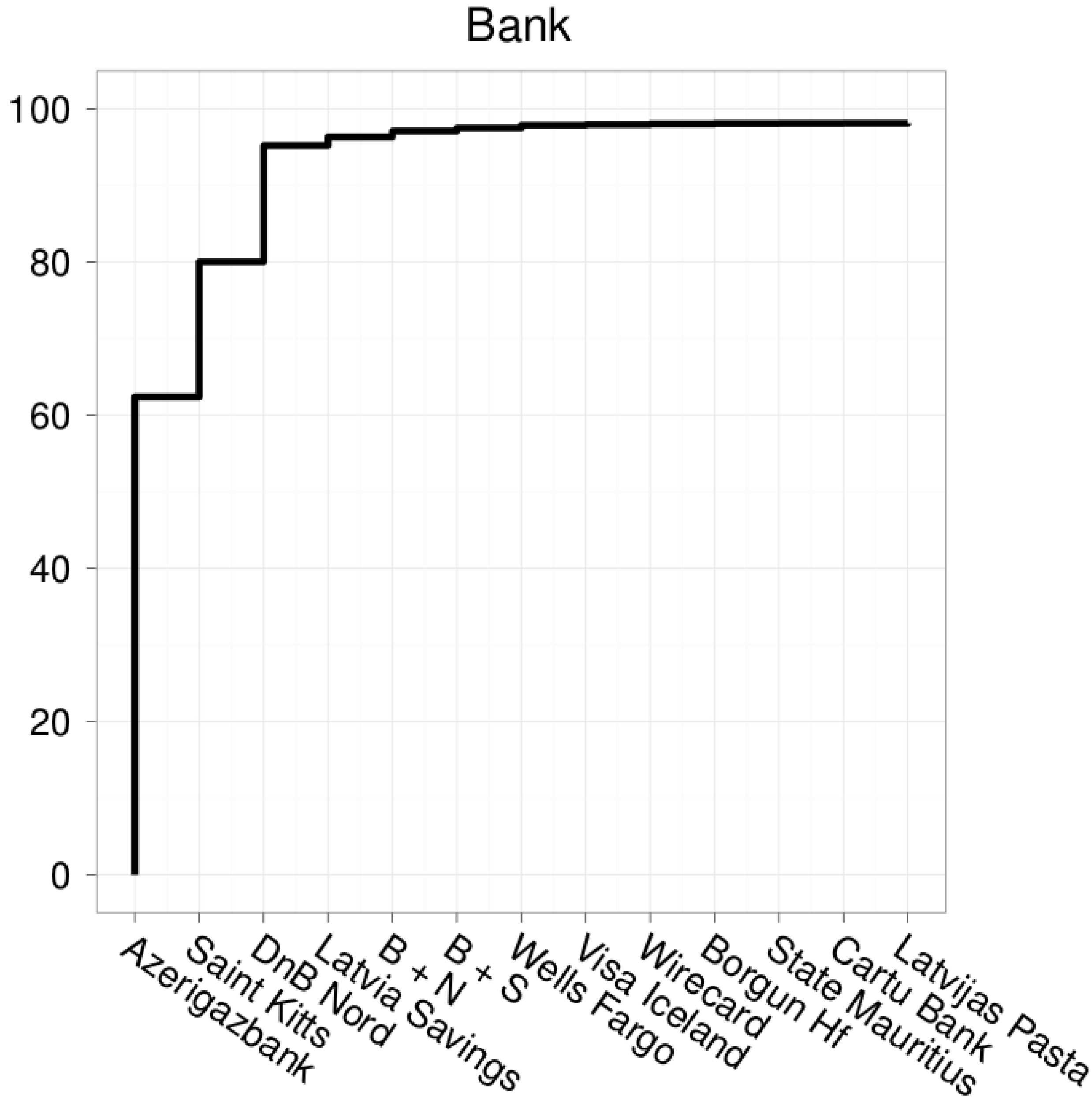
Web Hosters

DNS Server

Web Server



Banks



Bank
100
80
60
40
20
0
Azerigazbank
Saint Kitts
DnB Nord
Latvia Savings
B + N
B + S
Wells Fargo
Visa Iceland
Wirecard
Borgun Hf
State Mauritius
Cartu Bank
Latvijas Pasta

Switching a bank...

Requires coordination with:

- Bank
- VISA MasterCard
- Payment Processor

...and usually takes days or weeks!

Banks are the primary Bottleneck!

--- Commercial Break ---

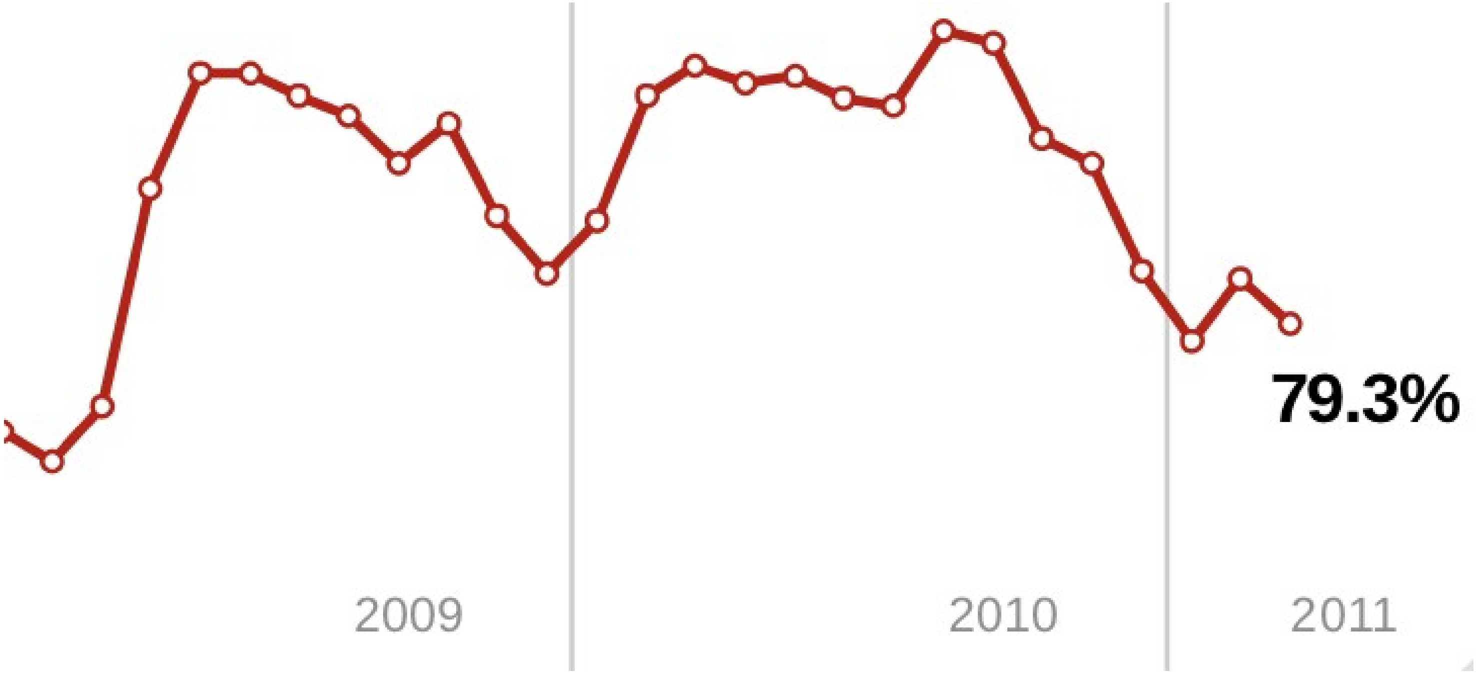
more curious stuff about spam

The CO_2 Footprint of Spam

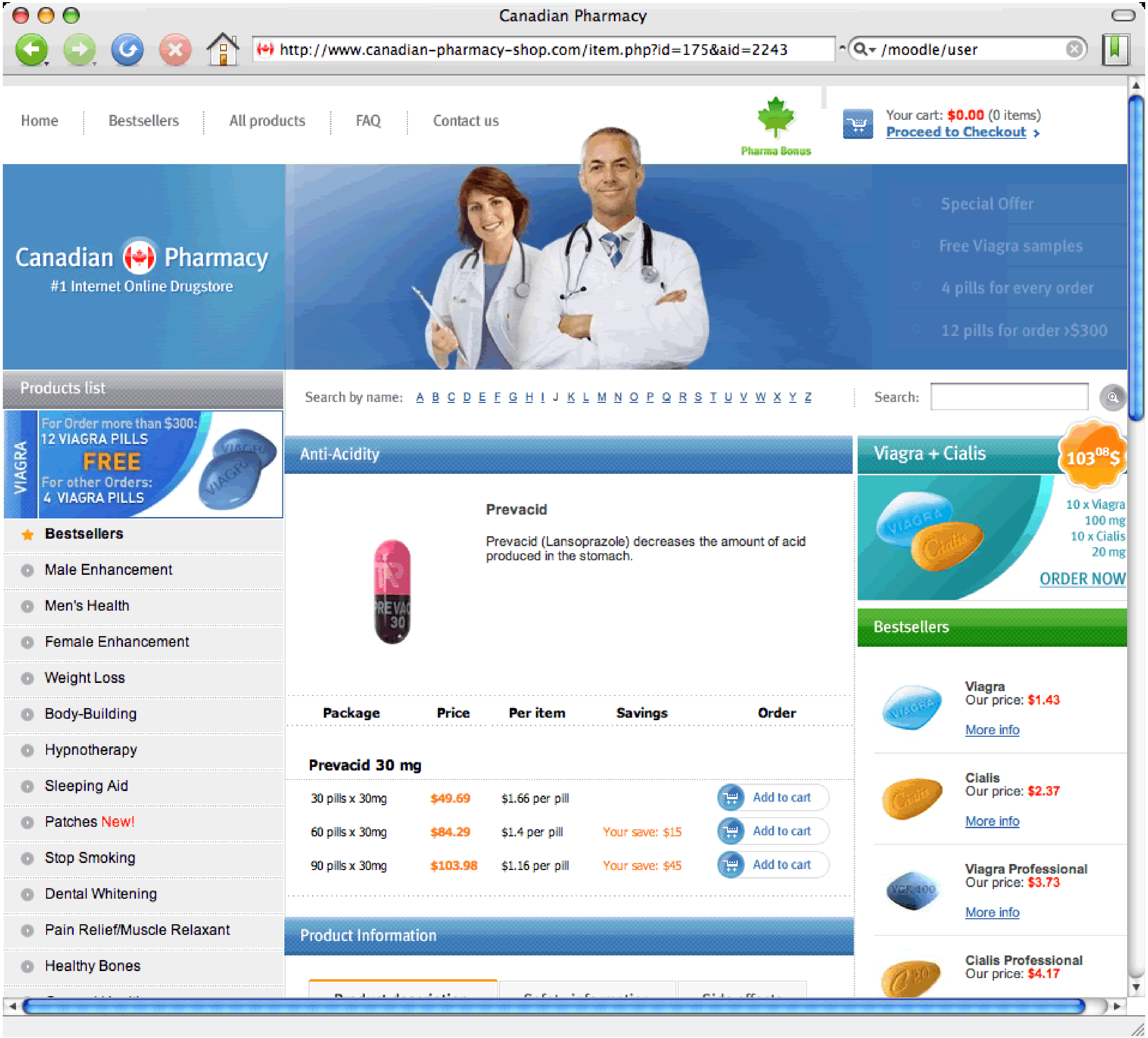
Annual global spam energy consumption could power 2.4 mio. US homes ≈ Chicago City

Source: McAfee: The Carbon Footprint of Spam

>= 80% of all email communication worldwide is spam



Source: MessageLab March 2011 Intelligence Report



Anti-Acidity

Prevacid

Prevacid (Lansoprazole) decreases the amount of acid produced in the stomach.

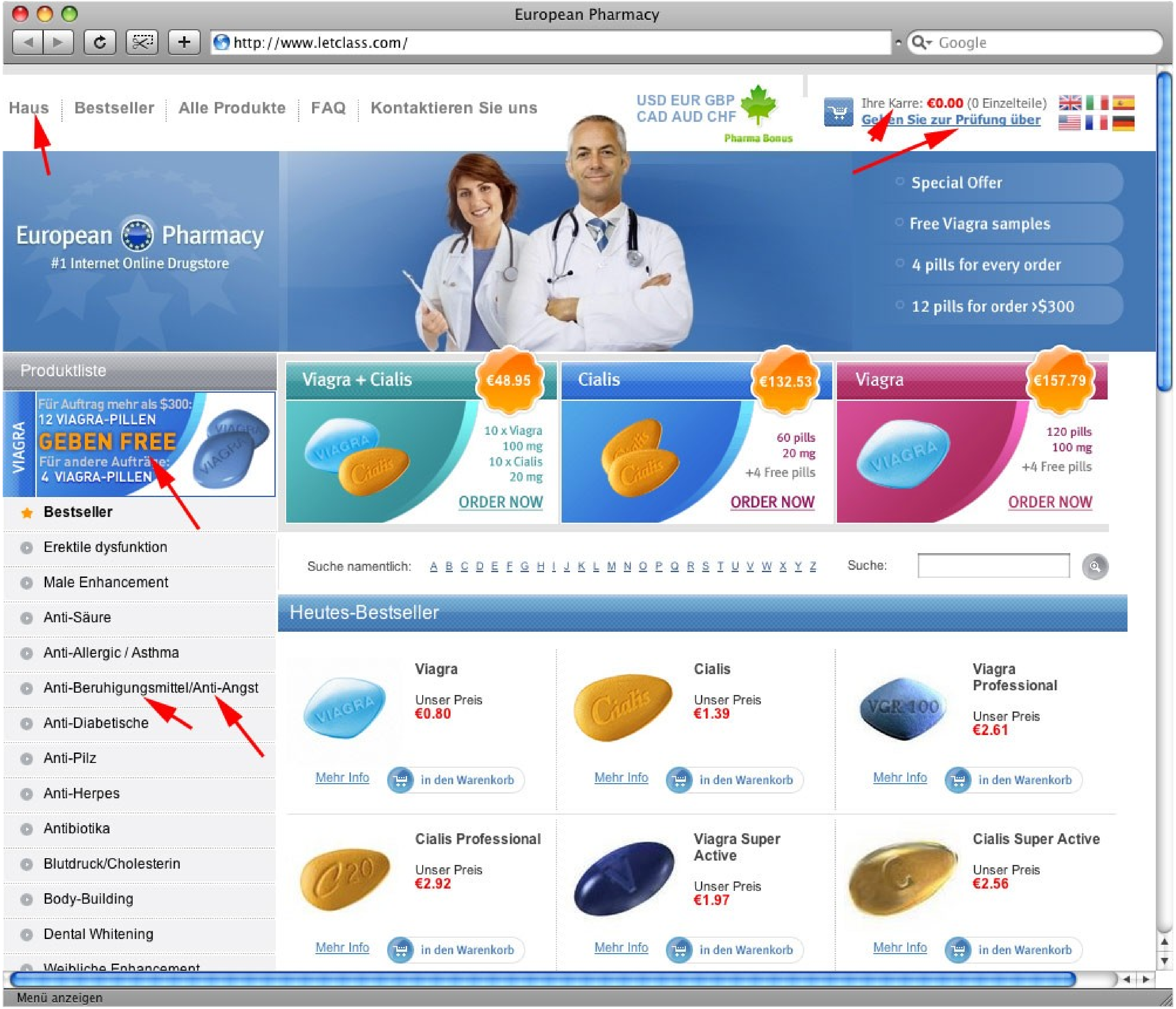
Package	Price	Per item	Savings	Order
Prevacid 30 mg				
30 pills x 30mg	$49.69	$1.66 per pill		Add to cart
60 pills x 30mg	$84.29	$1.4 per pill	Your save: $15	Add to cart
90 pills x 30mg	$103.98	$1.16 per pill	Your save: $45	Add to cart

Viagra
Our price: $1.43
More info

Cialis
Our price: $2.37
More info

Viagra Professional
Our price: $3.73
More info

Cialis Professional
Our price: $4.17



European Pharmacy

http://www.letclass.com/

Google

Haus | Bestseller | Alle Produkte | FAQ | Kontaktieren Sie uns

USD EUR GBP
CAD AUD CHF

Pharma Bonus

Ihre Karre: €0.00 (0 Einzelteile)
Gehen Sie zur Prüfung über

European Pharmacy
#1 Internet Online Drugstore

- Special Offer
- Free Viagra samples
- 4 pills for every order
- 12 pills for order >$300

Produktliste

VIAGRA
Für Auftrag mehr als $300:
12 VIAGRA-PILLEN
GEBEN FREE
Für andere Aufträge:
4 VIAGRA-PILLEN

Viagra + Cialis €48.95
10 x Viagra
100 mg
10 x Cialis
20 mg
ORDER NOW

Cialis €132.53
60 pills
20 mg
+4 Free pills
ORDER NOW

Viagra €157.79
120 pills
100 mg
+4 Free pills
ORDER NOW

- Bestseller
- Erektile dysfunktion
- Male Enhancement
- Anti-Säure
- Anti-Allergic / Asthma
- Anti-Beruhigungsmittel/Anti-Angst
- Anti-Diabetische
- Anti-Pilz
- Anti-Herpes
- Antibiotika
- Blutdruck/Cholesterin
- Body-Building
- Dental Whitening
- Weibliche Enhancement

Suche namentlich: 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

Suche:

Heutes-Bestseller

Viagra
Unser Preis
€0.80
Mehr Info | in den Warenkorb

Cialis
Unser Preis
€1.39
Mehr Info | in den Warenkorb

Viagra Professional
Unser Preis
€2.61
Mehr Info | in den Warenkorb

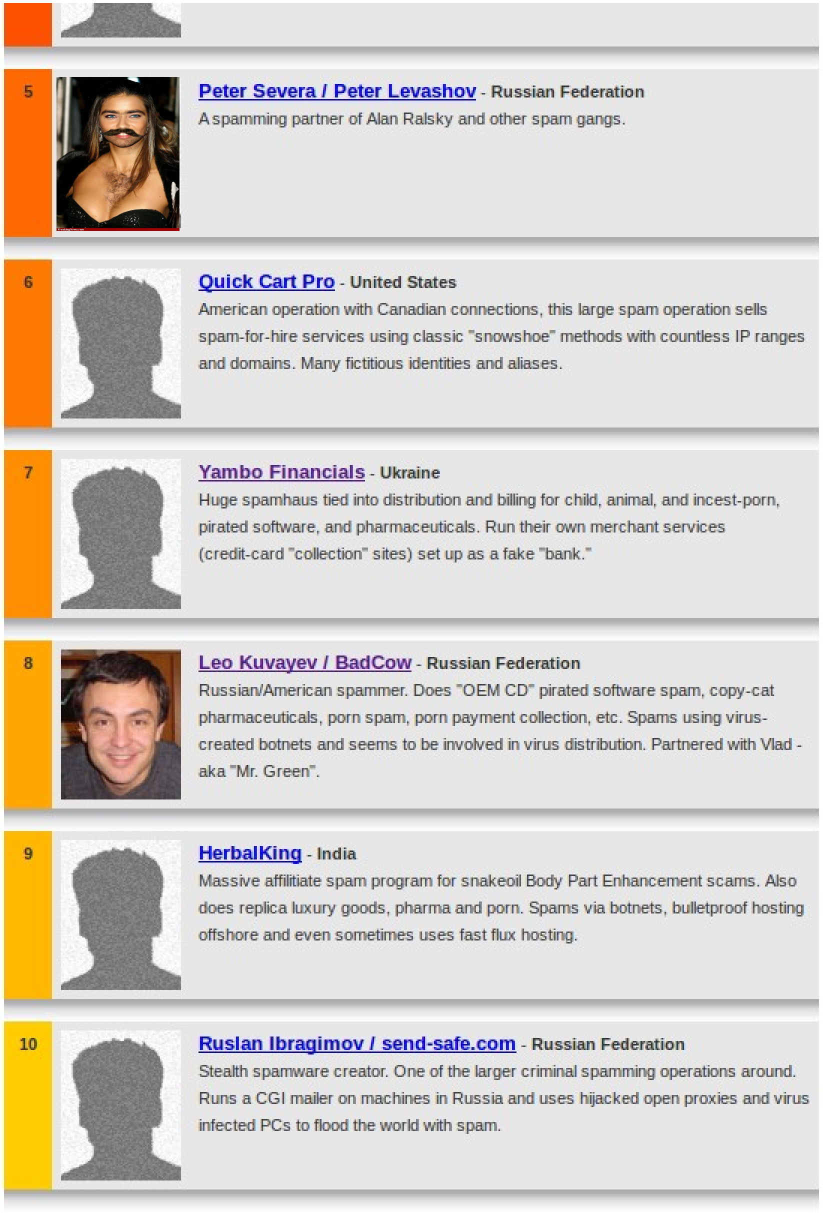
Cialis Professional
Unser Preis
€2.92
Mehr Info | in den Warenkorb

Viagra Super Active
Unser Preis
€1.97
Mehr Info | in den Warenkorb

Cialis Super Active
Unser Preis
€2.56
Mehr Info | in den Warenkorb

Menü anzeigen

ROKSO (Register Of Known Spam Operations)



5 **Peter Severa / Peter Levashov** - Russian Federation
A spamming partner of Alan Ralsky and other spam gangs.

6 **Quick Cart Pro** - United States
American operation with Canadian connections, this large spam operation sells spam-for-hire services using classic "snowshoe" methods with countless IP ranges and domains. Many fictitious identities and aliases.

7 **Yambo Financials** - Ukraine
Huge spamhaus tied into distribution and billing for child, animal, and incest-porn, pirated software, and pharmaceuticals. Run their own merchant services (credit-card "collection" sites) set up as a fake "bank."

8 **Leo Kuvayev / BadCow** - Russian Federation
Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green".

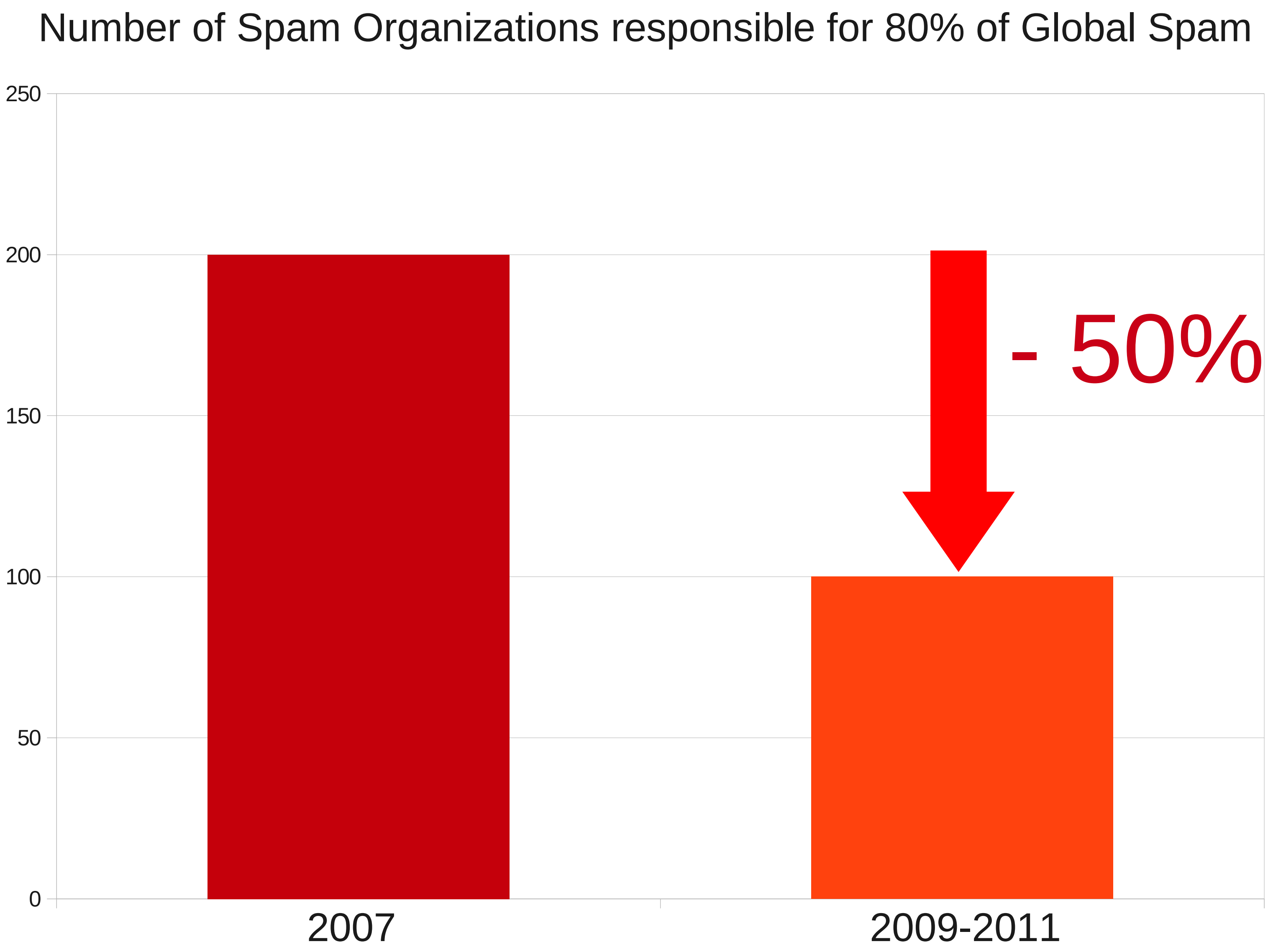
9 **HerbalKing** - India
Massive affiliate spam program for snakeoil Body Part Enhancement scams. Also does replica luxury goods, pharma and porn. Spams via botnets, bulletproof hosting offshore and even sometimes uses fast flux hosting.

10 **Ruslan Ibragimov / send-safe.com** - Russian Federation
Stealth spamware creator. One of the larger criminal spamming operations around. Runs a CGI mailer on machines in Russia and uses hijacked open proxies and virus infected PCs to flood the world with spam.

- Lists known professional spam organizations and individuals
- A lot of spammers are actually known!

Source: http://www.spamhaus.org/rokso/

Spam Concentration

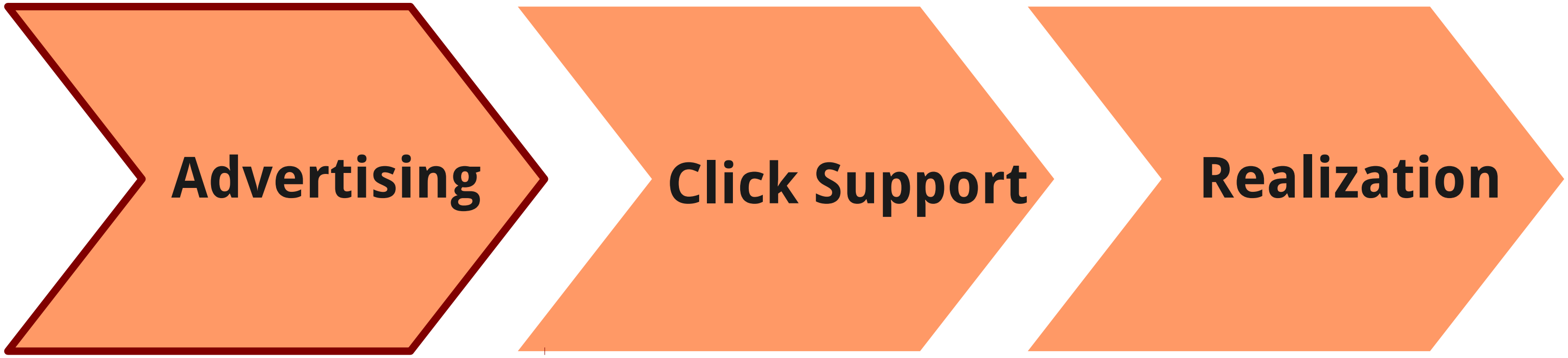


Source: http://www.spamhaus.org/rokso/

End of Commercial Break

(serious stuff from now on)

Judo: ”Fighting Spam with itself”



Advertising

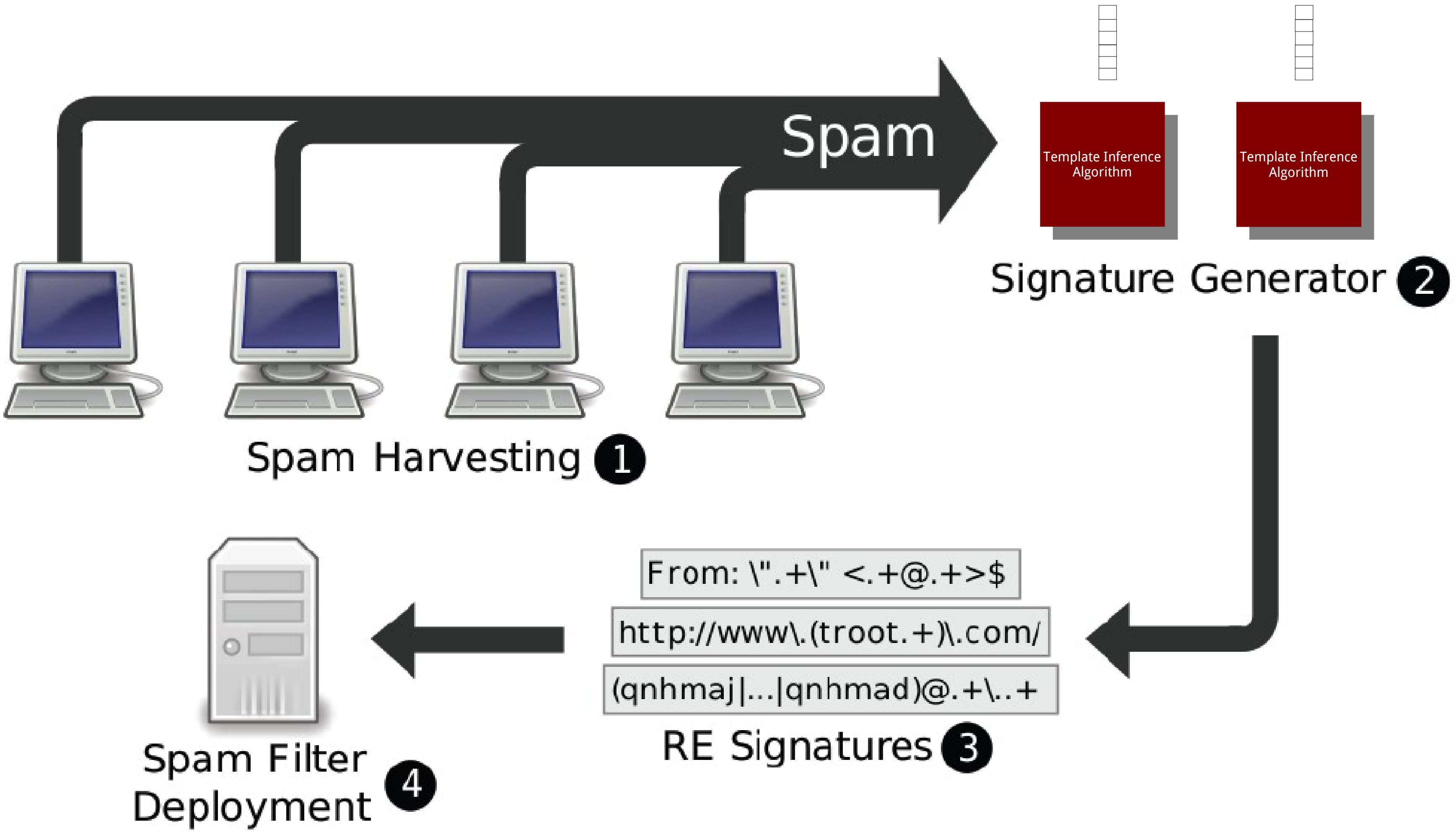
Click Support

Realization

Traditional Spam Fighting

- **Vantage Point: Receiver**
  - e.g. Received the same mail 100k times → must be spam
  - URL Domain Blacklisting
  - Subject-line Blacklisting

Judo's Vantage Point: Source



Spam

Template Inference Algorithm

Template Inference Algorithm

Signature Generator 2

Spam Harvesting 1

From: \".+\" <.+@.+>$

http://www\.(troot.+)\.com/

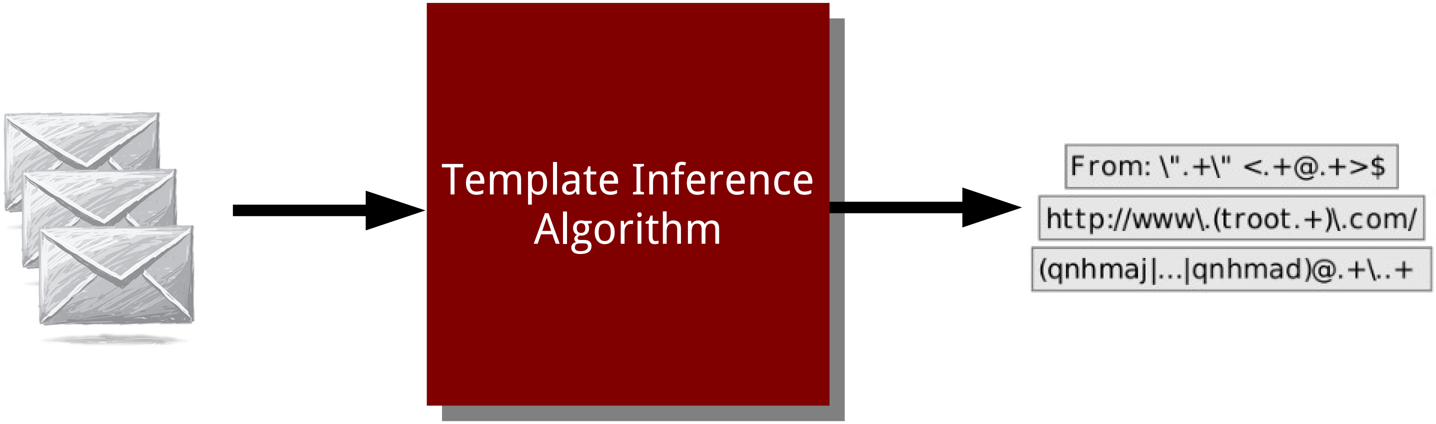
(qnhmaj|...|qnhmad)@.+\..+

RE Signatures 3

Spam Filter Deployment 4

I.e., use your private botfarm to harvest spam.

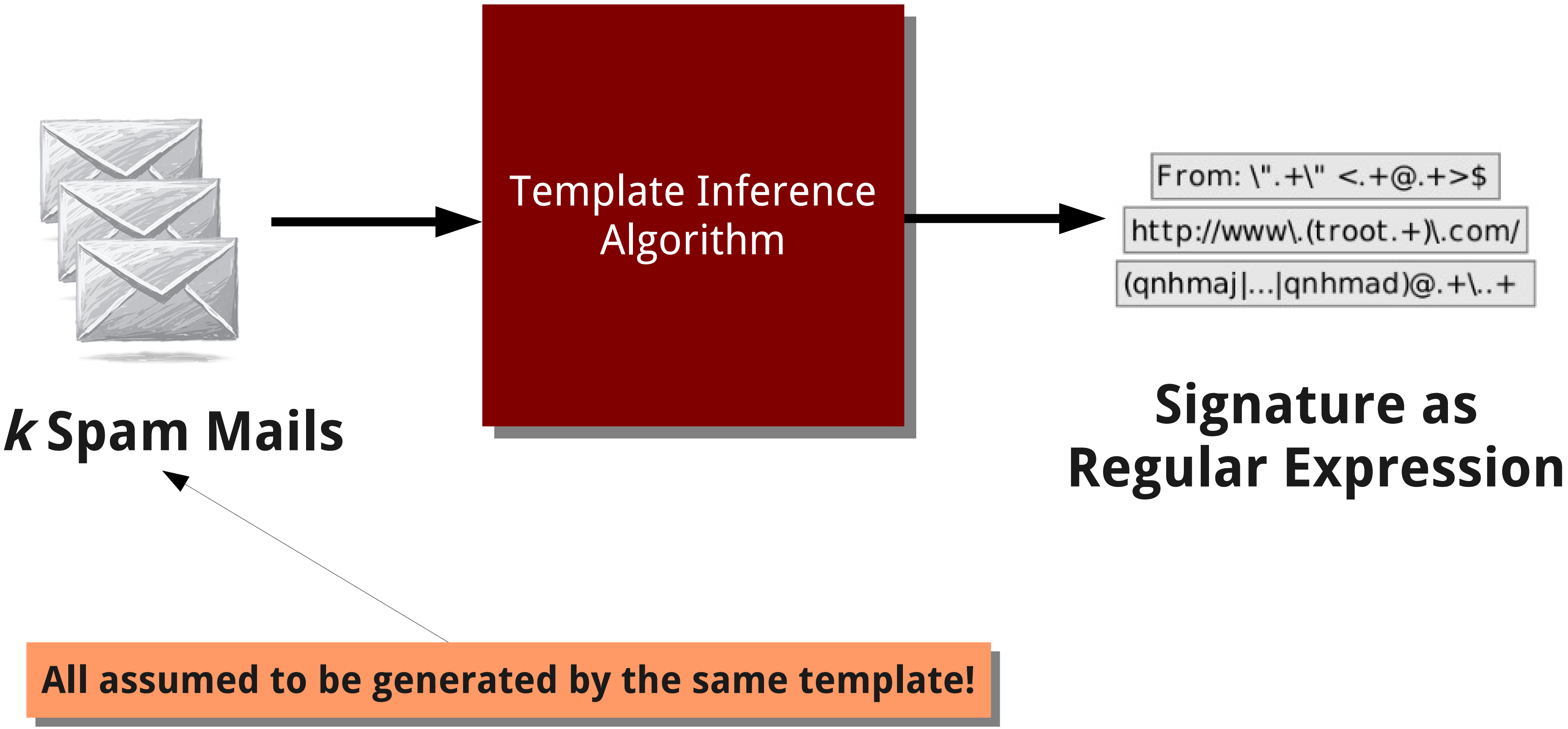
Single Template Inference



Template Inference Algorithm

```
From: \".+\" <.+@.+>$
http://www\.(troot.+)\.com/
(qnhmaj|...|qnhmad)@.+\..+
```

Single Template Inference



k Spam Mails

Template Inference Algorithm

```
From: \".+\" <.+@.+>$
http://www\.(troot.+)\.com/
(qnhmaj|...|qnhmad)@.+\..+
```

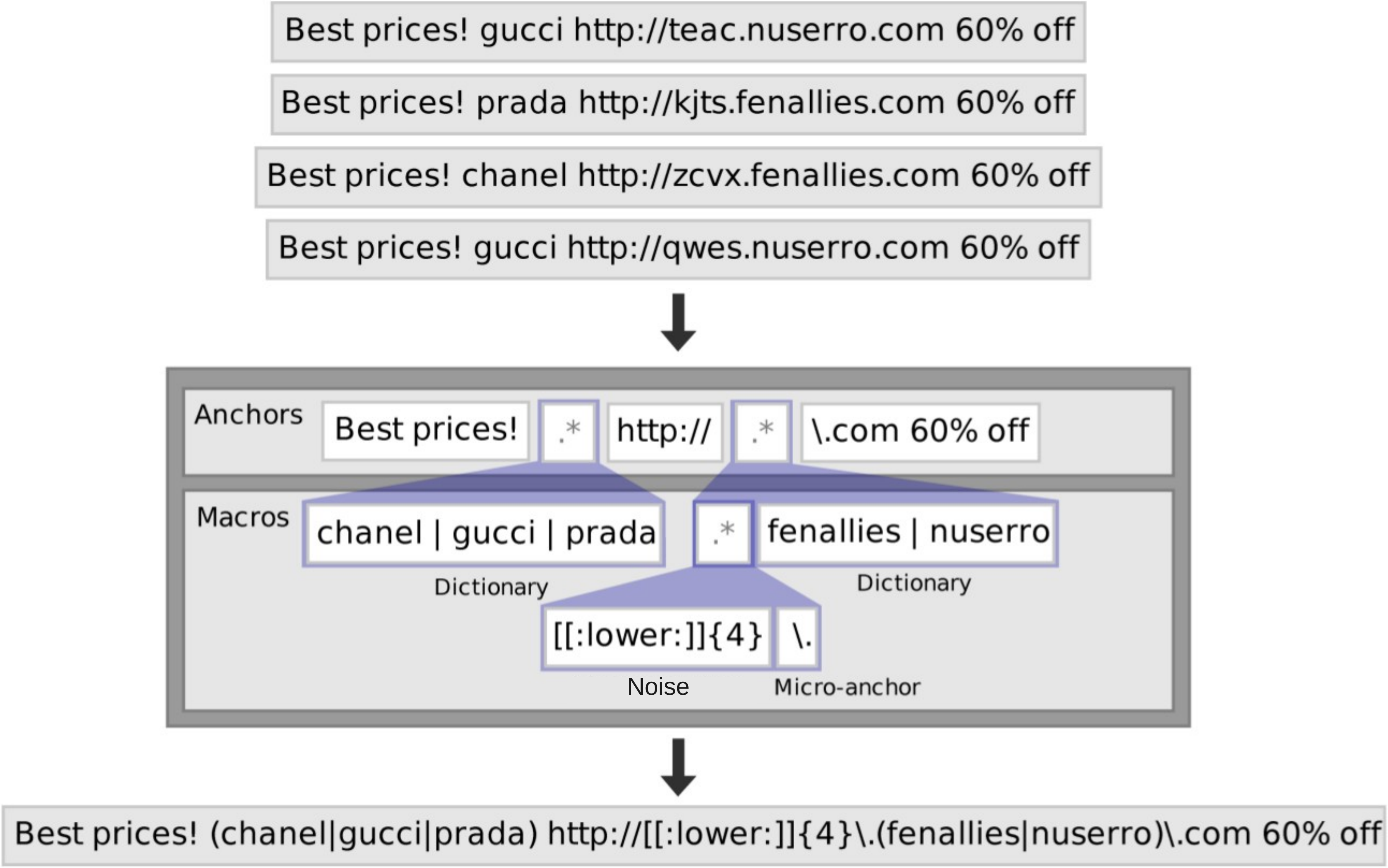
Signature as Regular Expression

All assumed to be generated by the same template!

Building Blocks of Judo Signatures

- Anchors: invariant strings: `http://`,
  - Micro-Anchors: `@ , . :` …
- Macros: variant strings
  - Dictionary-based: `chanel` | `gucci` | `prada`
  - Noise Macros: `zvcx`, `qwsy`, …

An Example Judo Signature



Best prices! gucci http://teac.nuserro.com 60% off

Best prices! prada http://kjts.fenallies.com 60% off

Best prices! chanel http://zcvx.fenallies.com 60% off

Best prices! gucci http://qwes.nuserro.com 60% off

Best prices! (chanel|gucci|prada) http://[[:lower:]]{4}\.(fenallies|nuserro)\.com 60% off

Source: Botnet Judo – Fighting Spam with Itself

Template Inference Algorithm

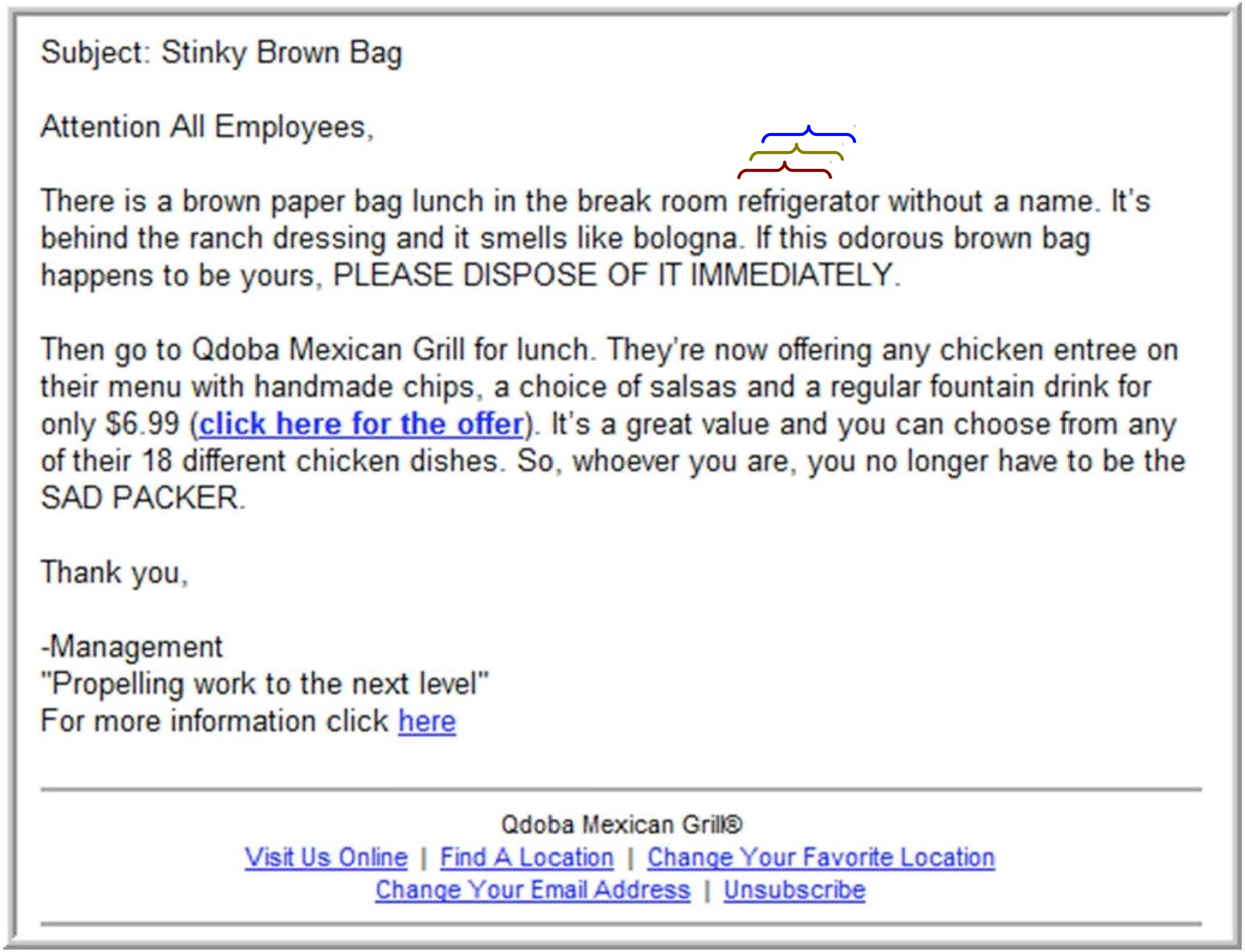
1. Learn Anchors `http://`
2. Learn Macros (= text between Anchors)
    1. Dictionary Macros `chanel` | `gucci` | `prada`
    2. Micro Anchors `@ . , ;`
    3. Noise Macros (= the ”rest”) `zvcx`, `qwsy`

Learning Anchors

1. Sequence of substrings **Σ** ← Slide window of length *q* over each message

2. Set of Anchors **A** ← Compute the Longest Common Subsequence (LCS) over **Σ**

Sliding Window of Length *q*



Subject: Stinky Brown Bag

Attention All Employees,

There is a brown paper bag lunch in the break room refrigerator without a name. It's behind the ranch dressing and it smells like bologna. If this odorous brown bag happens to be yours, PLEASE DISPOSE OF IT IMMEDIATELY.

Then go to Qdoba Mexican Grill for lunch. They're now offering any chicken entree on their menu with handmade chips, a choice of salsas and a regular fountain drink for only $6.99 (**click here for the offer**). It's a great value and you can choose from any of their 18 different chicken dishes. So, whoever you are, you no longer have to be the SAD PACKER.

Thank you,

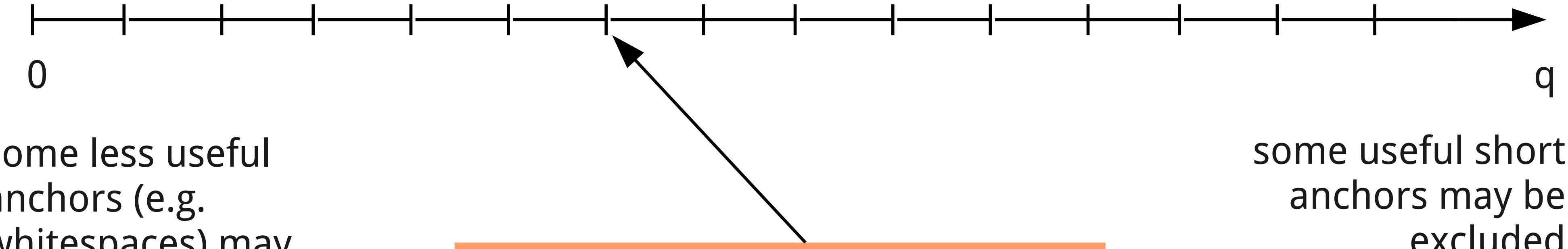
-Management
"Propelling work to the next level"
For more information click here

Qdoba Mexican Grill®
Visit Us Online | Find A Location | Change Your Favorite Location
Change Your Email Address | Unsubscribe

Selection of Parameter q

too small (e.g. 1):

too large:



some less useful anchors (e.g. whitespaces) may be included

some useful short anchors may be excluded

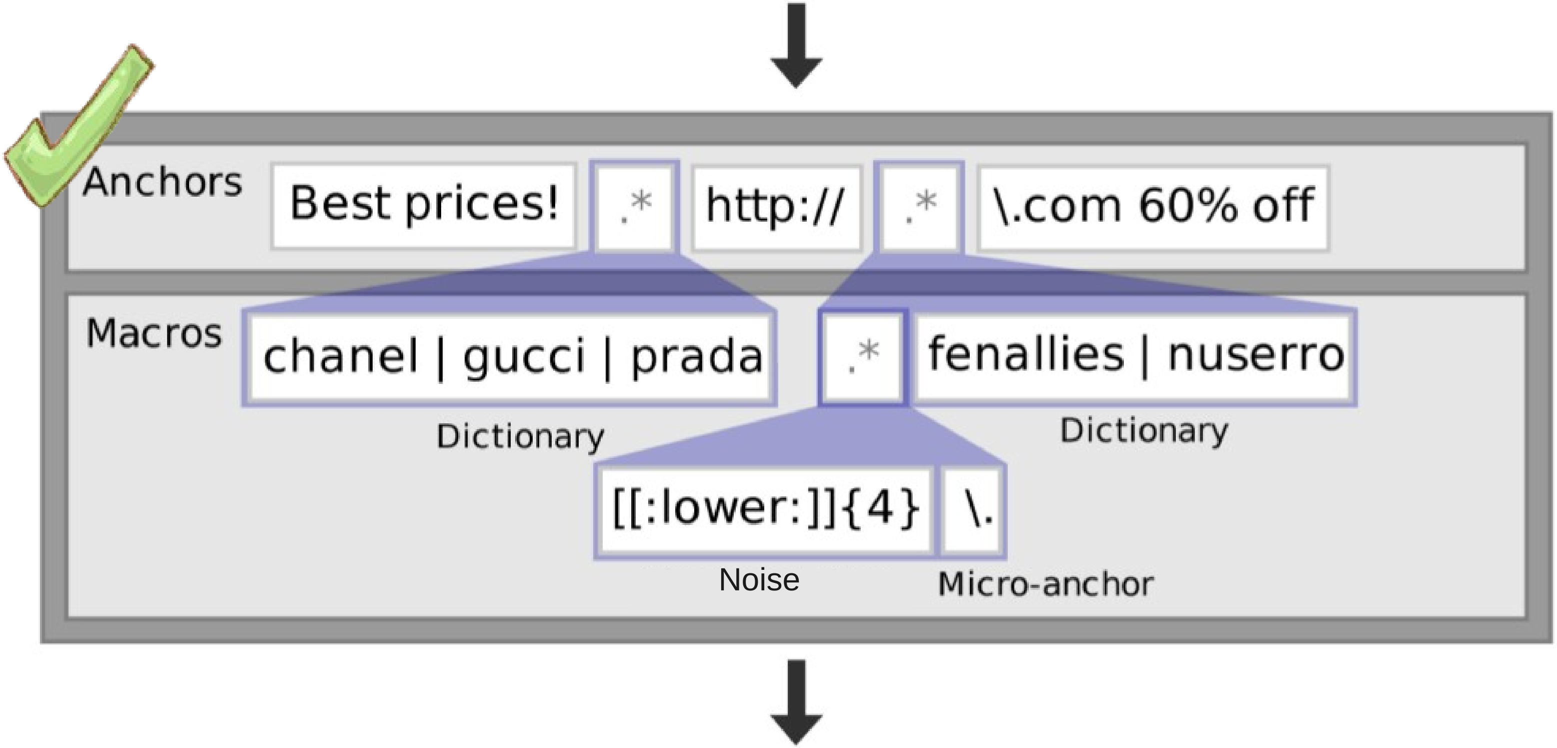
Empirical evidence suggests *q* = 6

Best prices! gucci http://teac.nuserro.com 60% off

Best prices! prada http://kjts.fenallies.com 60% off

Best prices! chanel http://zcvx.fenallies.com 60% off

Best prices! gucci http://qwes.nuserro.com 60% off



Anchors

Best prices! .* http:// .* \.com 60% off

Macros

chanel | gucci | prada

Dictionary

.*

fenallies | nuserro

Dictionary

[[:lower:]]{4} \.

Noise

Micro-anchor

Best prices! (chanel|gucci|prada) http://[[:lower:]]{4}\.(fenallies|nuserro)\.com 60% off

Source: Botnet Judo – Fighting Spam with Itself

Learning Dictionary Macros

`chanel | gucci | prada`

Q: Have we seen all dictionary elements?

A: Use a statistical test with

0-Hypothesis:

"There still is an unobserved dictionary element"

✓

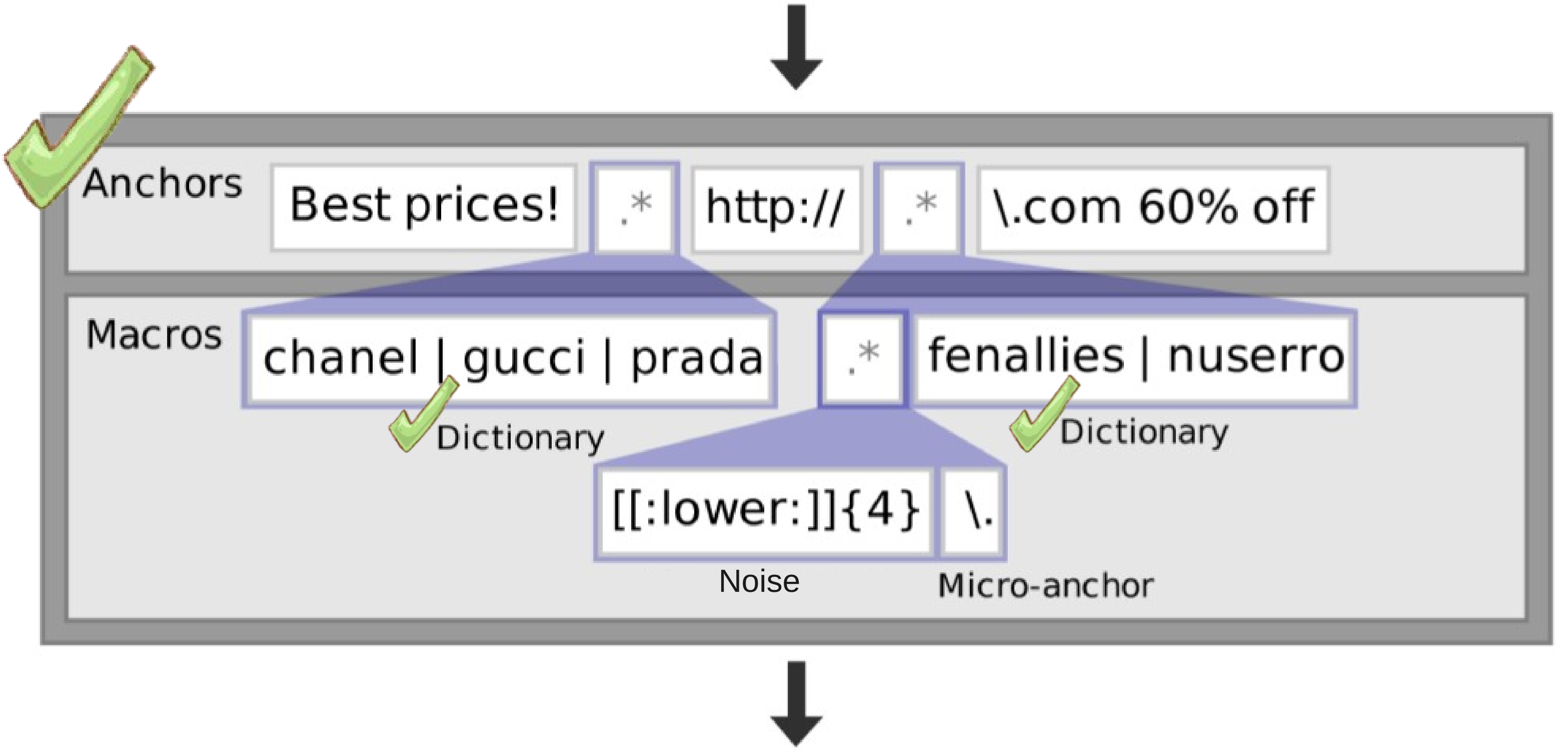
0-Hypothesis rejected → Very probably a dictionary macro.

Best prices! gucci http://teac.nuserro.com 60% off

Best prices! prada http://kjts.fenallies.com 60% off

Best prices! chanel http://zcvx.fenallies.com 60% off

Best prices! gucci http://qwes.nuserro.com 60% off



Anchors

Best prices! | .* | http:// | .* | \.com 60% off

Macros

chanel | gucci | prada

Dictionary

.*

fenallies | nuserro

Dictionary

[[:lower:]]{4} | \.

Noise

Micro-anchor

Best prices! (chanel|gucci|prada) http://[[:lower:]]{4}\.(fenallies|nuserro)\.com 60% off

Source: Botnet Judo – Fighting Spam with Itself

Learning Micro-Anchors @ , . :

If Dictionary Test fails: ✗

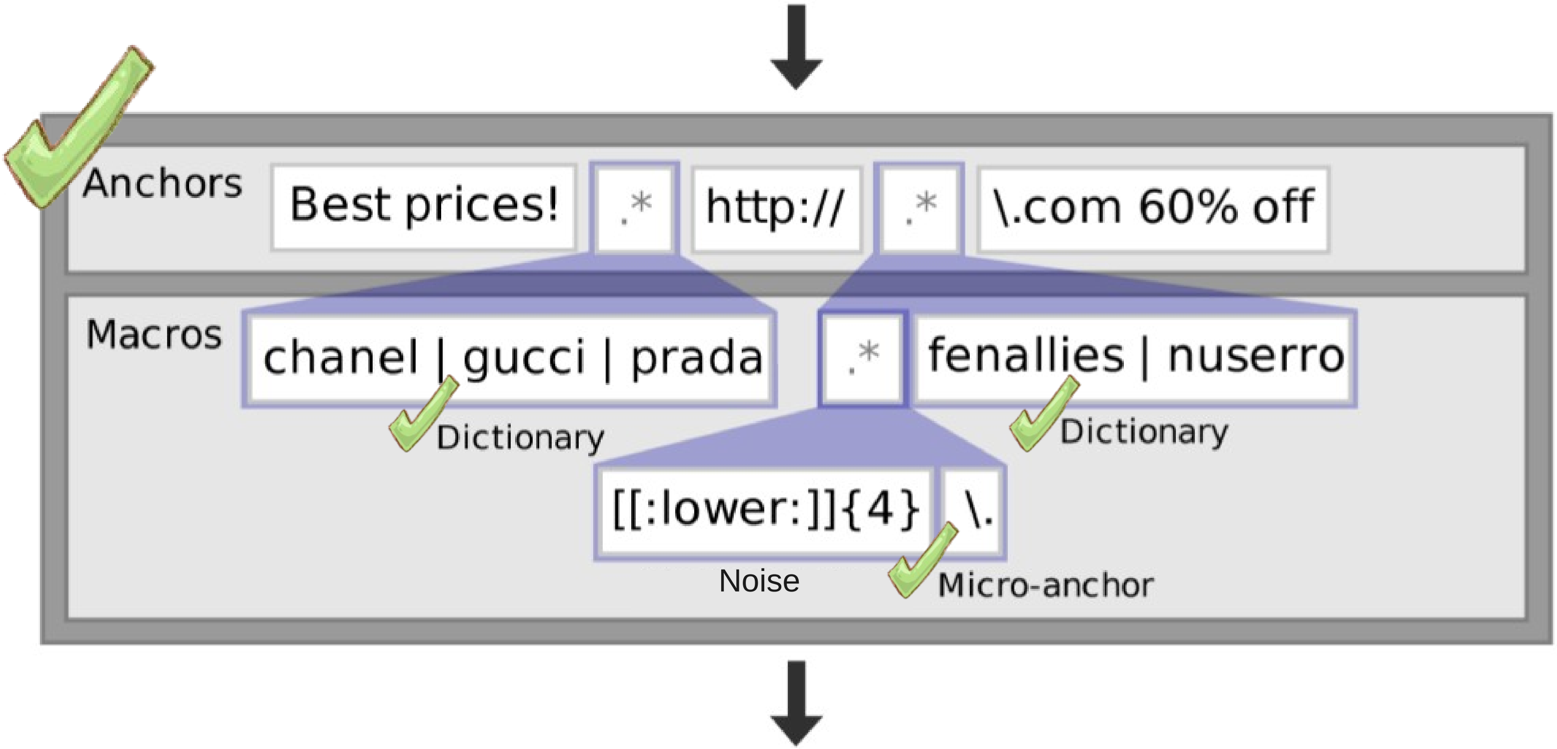
check if it's a Micro-Anchor using LCS but only allow non-alphanumeric chars (@ , . : etc.) to match.

Best prices! gucci http://teac.nuserro.com 60% off

Best prices! prada http://kjts.fenallies.com 60% off

Best prices! chanel http://zcvx.fenallies.com 60% off

Best prices! gucci http://qwes.nuserro.com 60% off



Anchors

Best prices! .* http:// .* \.com 60% off

Macros

chanel | gucci | prada

Dictionary

.*

fenallies | nuserro

Dictionary

[[:lower:]]{4} \.

Noise

Micro-anchor

Best prices! (chanel|gucci|prada) http://[[:lower:]]{4}\.(fenallies|nuserro)\.com 60% off

Source: Botnet Judo – Fighting Spam with Itself

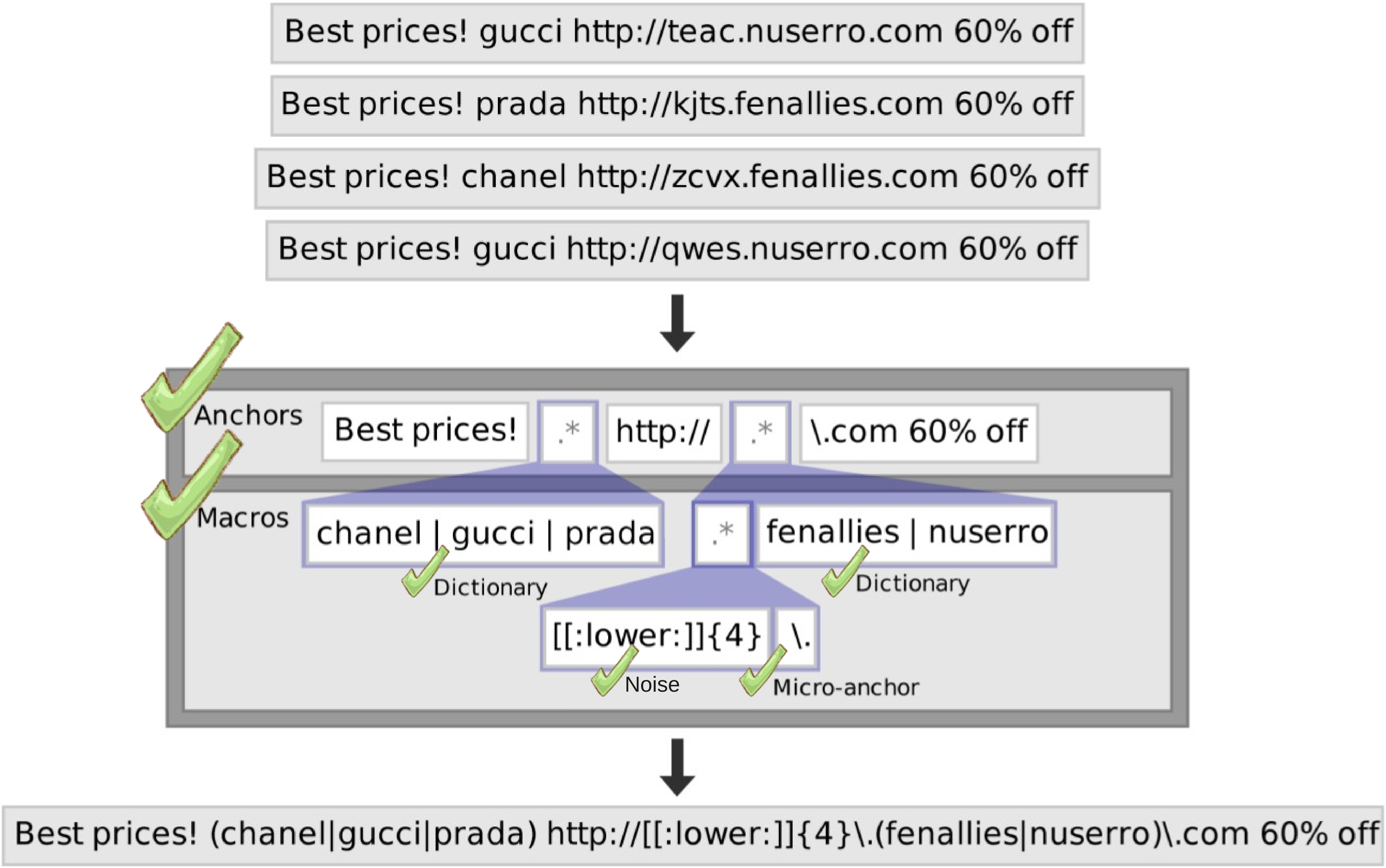
Learning Noise Macros `zvcx qwsy`

- Perform Dictionary Test on all elements delimited by Micro-Anchors

- Test fails: ❌
  → Noise Macro

- Representation:

`zvcx qwsy` ⇔ `[[:lower:]]{4}`



Best prices! gucci http://teac.nuserro.com 60% off

Best prices! prada http://kjts.fenallies.com 60% off

Best prices! chanel http://zcvx.fenallies.com 60% off

Best prices! gucci http://qwes.nuserro.com 60% off

Anchors

Best prices! | .* | http:// | .* | \.com 60% off

Macros

chanel | gucci | prada

Dictionary

.*

fenallies | nuserro

Dictionary

[[:lower:]]{4} | \.

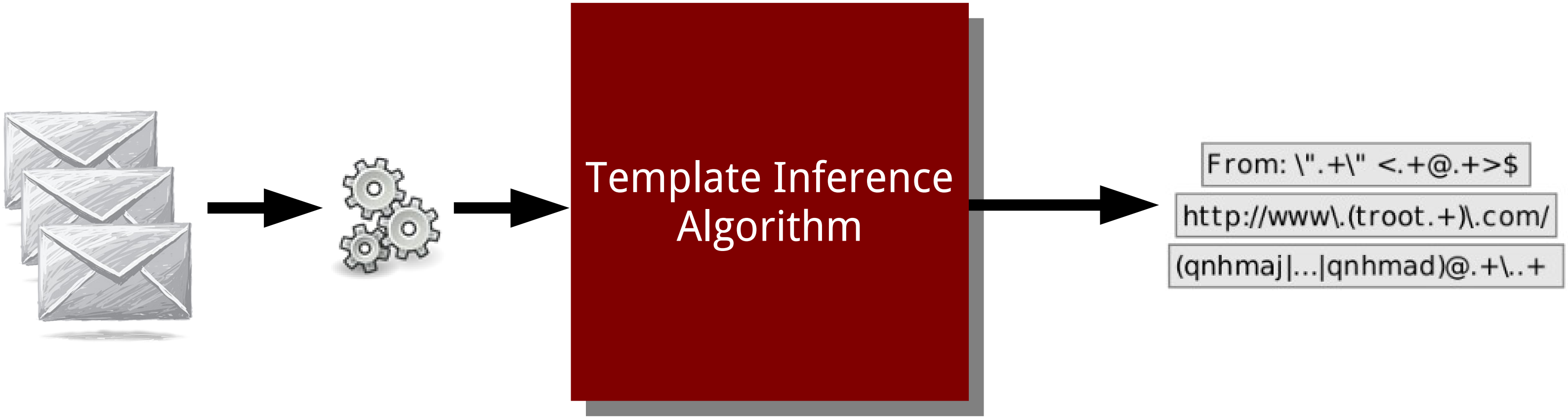
Noise

Micro-anchor

Best prices! (chanel|gucci|prada) http://[[:lower:]]{4}\.(fenallies|nuserro)\.com 60% off

Source: Botnet Judo – Fighting Spam with Itself

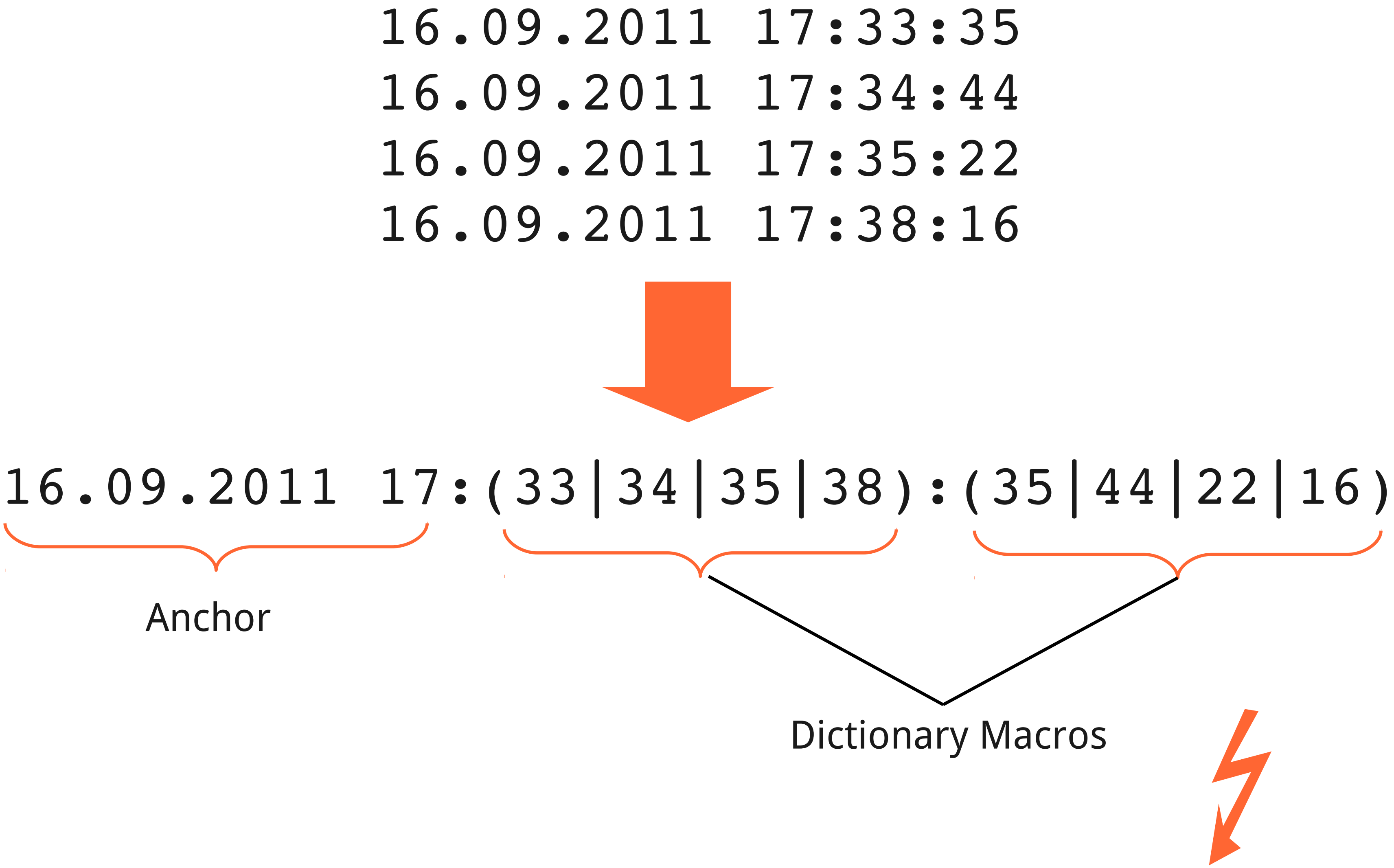
(Selected) Pre-Processing



Template Inference Algorithm

```
From: \".+\" <.+@.+>$
http://www\.(troot.+)\.com/
(qnhmaj|...|qnhmad)@.+\..+
```

Special Tokens



```
16.09.2011 17:33:35
16.09.2011 17:34:44
16.09.2011 17:35:22
16.09.2011 17:38:16
```

```
16.09.2011 17:(33|34|35|38):(35|44|22|16)
```

Anchor

Dictionary Macros

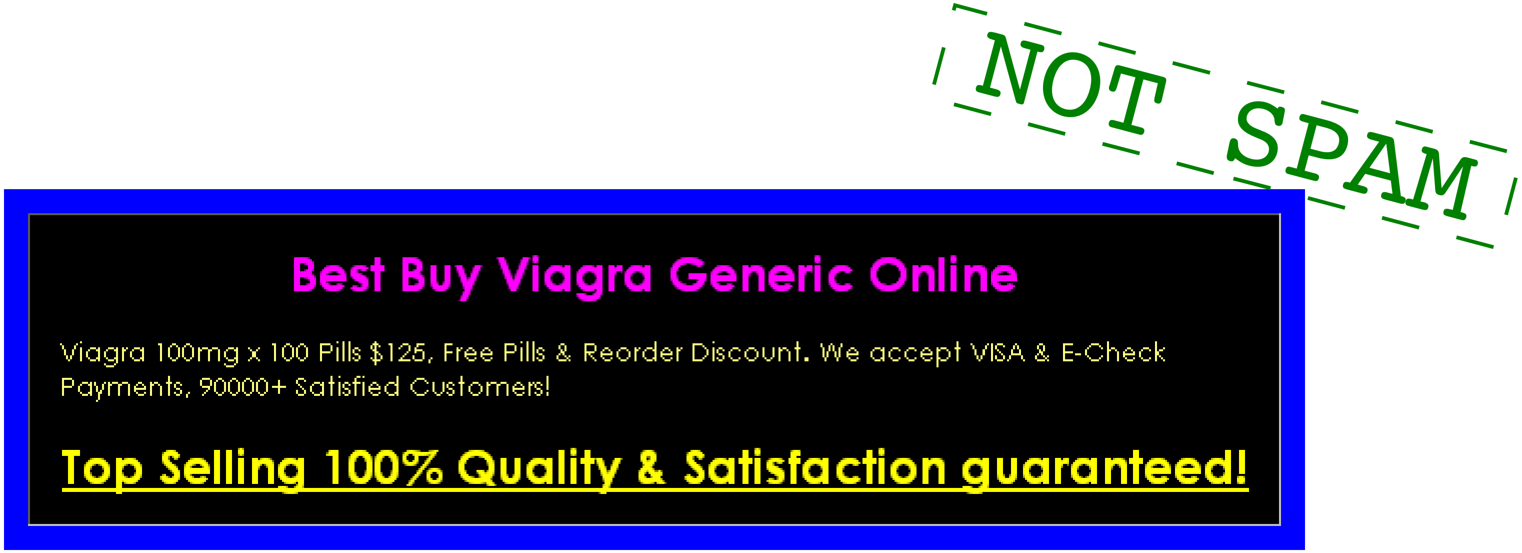
Workaround

- Dates
- IP addresses
- Multi-part message delimiters

...are treated as fixed Anchors
during Learning Phase.

Once signature is learned,
fixed Anchors are turned into a RegEx.

Effectiveness: False Negative Rate



NOT SPAM

Best Buy Viagra Generic Online

Viagra 100mg x 100 Pills $125, Free Pills & Reorder Discount. We accept VISA & E-Check Payments, 90000+ Satisfied Customers!

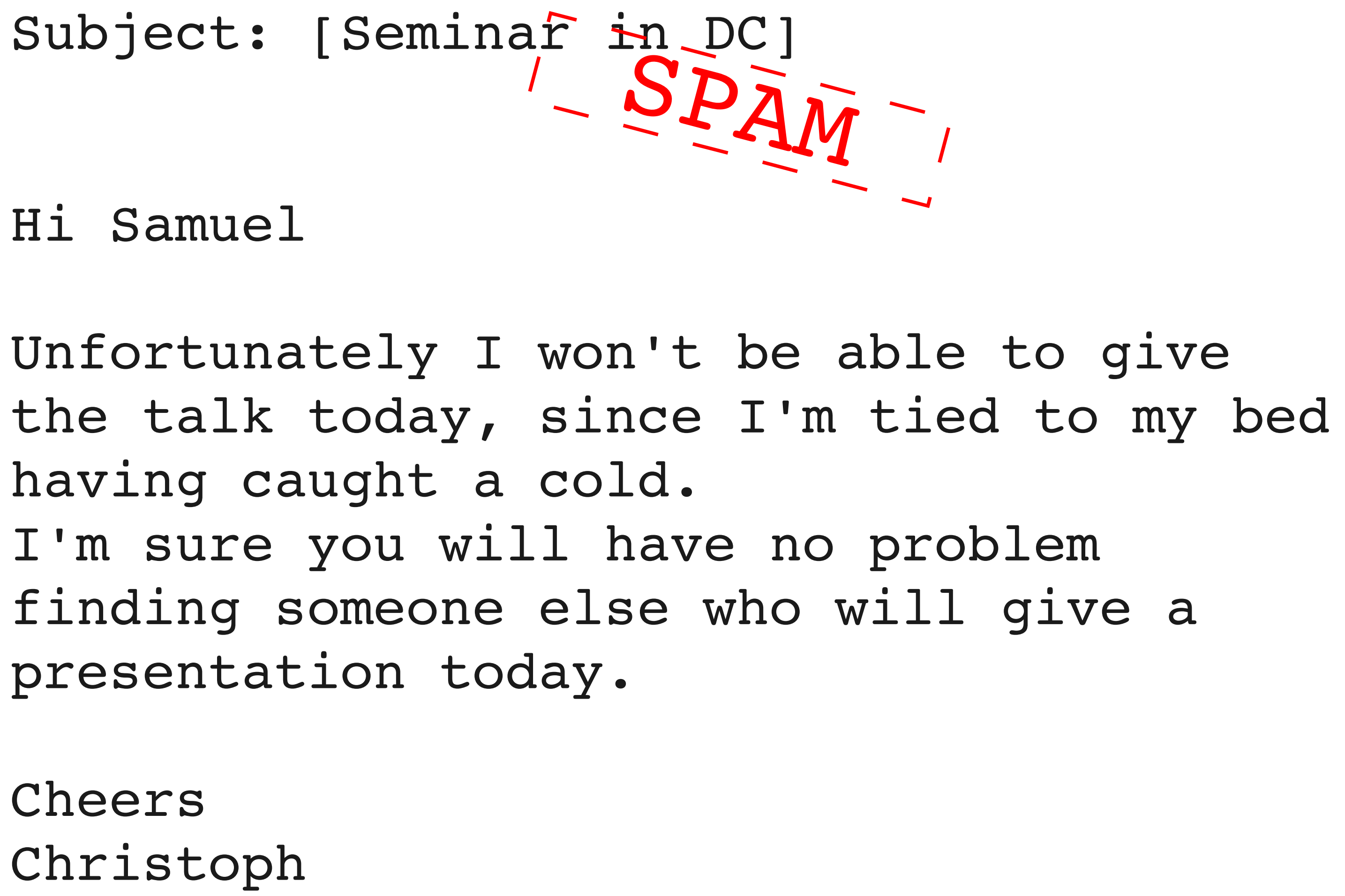
Top Selling 100% Quality & Satisfaction guaranteed!

Single Template Inference - Effectiveness

With k=50, 99% of templates were already captured perfectly, i.e. with **0 False Negatives**!

Need k=1000 to achieve same result!

Safety: False Positive Rate



Subject: [Seminar in DC]

SPAM

Hi Samuel

Unfortunately I won't be able to give
the talk today, since I'm tied to my bed
having caught a cold.
I'm sure you will have no problem
finding someone else who will give a
presentation today.

Cheers
Christoph

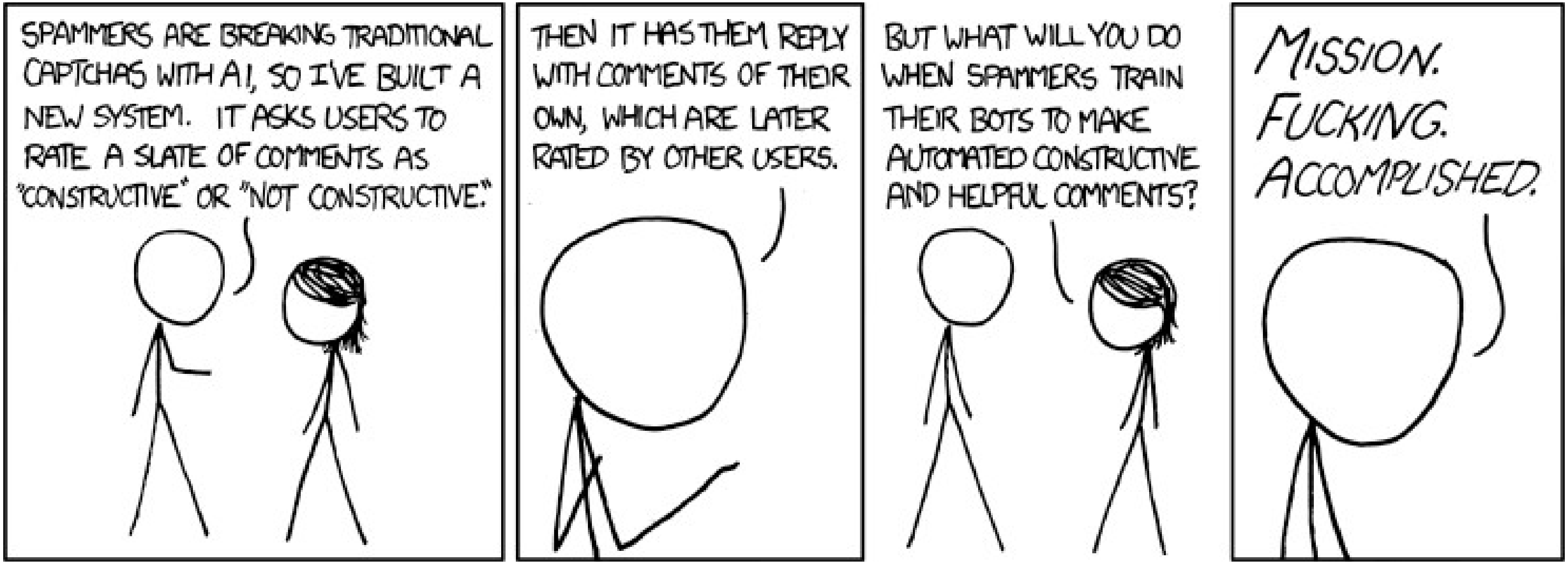
The Safety of Judo is due to...

...using Headers + Body (**extensive** information)

...forcing a signature to have Dictionary Macros and Anchors (very **restrictive**)

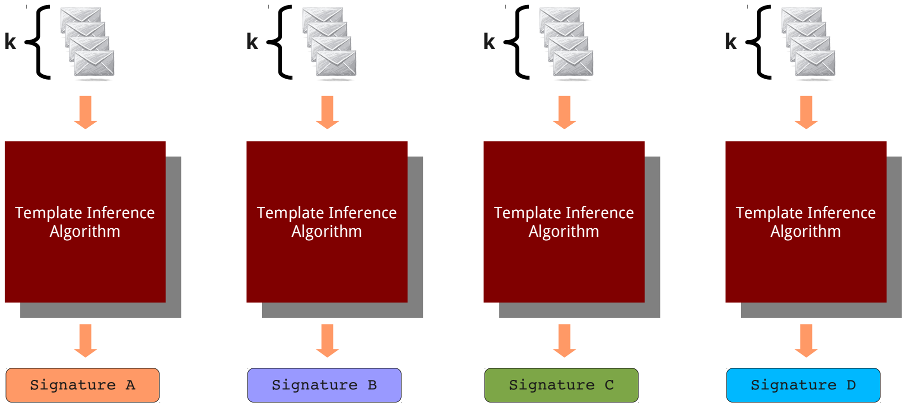
Summary

$$

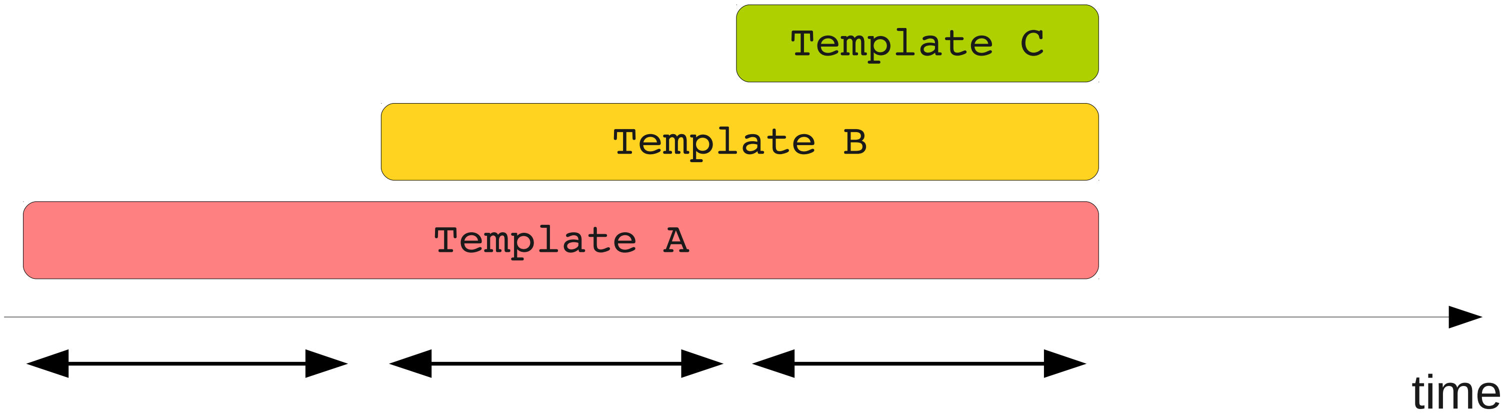

SPAMMERS ARE BREAKING TRADITIONAL CAPTCHAS WITH A.I., SO I'VE BUILT A NEW SYSTEM. IT ASKS USERS TO RATE A SLATE OF COMMENTS AS "CONSTRUCTIVE" OR "NOT CONSTRUCTIVE."
THEN IT HAS THEM REPLY WITH COMMENTS OF THEIR OWN, WHICH ARE LATER RATED BY OTHER USERS.
BUT WHAT WILL YOU DO WHEN SPAMMERS TRAIN THEIR BOTS TO MAKE AUTOMATED CONSTRUCTIVE AND HELPFUL COMMENTS?
MISSION. FUCKING. ACCOMPLISHED.

Source: xkcd

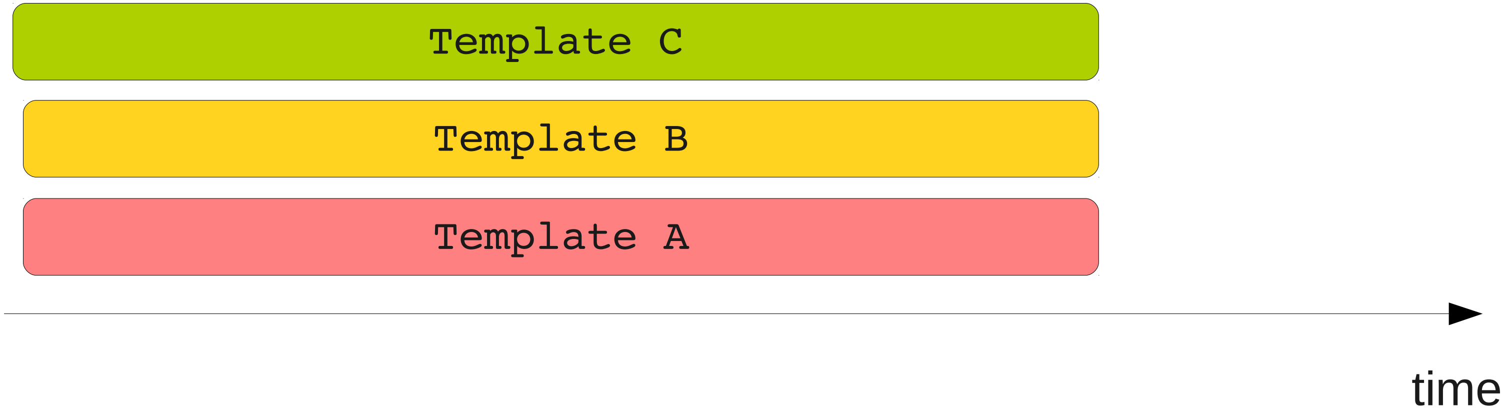
Multiple Template Inference


k
k
k
k
Template Inference Algorithm
Template Inference Algorithm
Template Inference Algorithm
Template Inference Algorithm
Signature A
Signature B
Signature C
Signature D

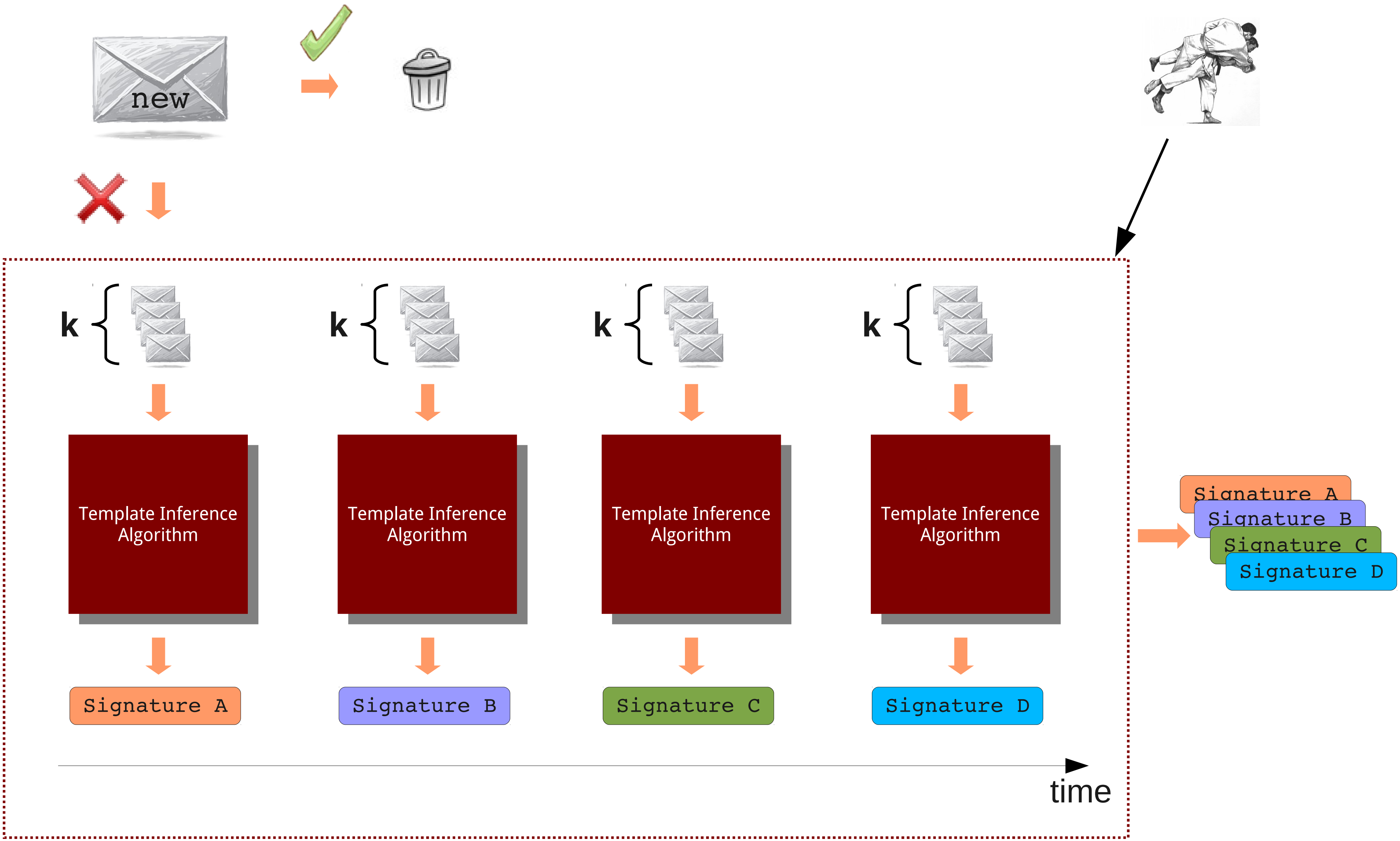
Assumption: Incremental Template Deployment



And not:



Multiple Template Inference



new

k

Template Inference Algorithm

Signature A

k

Template Inference Algorithm

Signature B

k

Template Inference Algorithm

Signature C

k

Template Inference Algorithm

Signature D

time

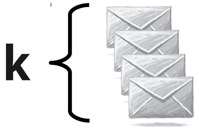
Signature A

Signature B

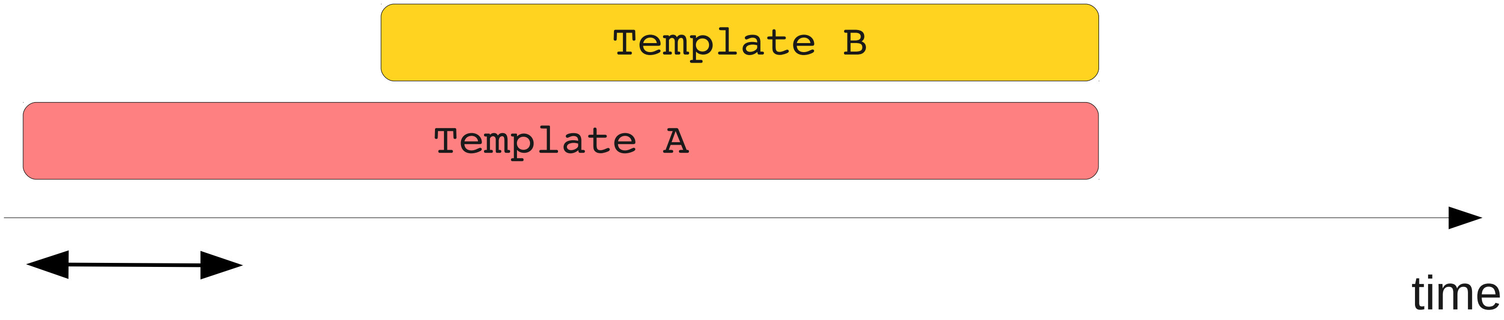
Signature C

Signature D

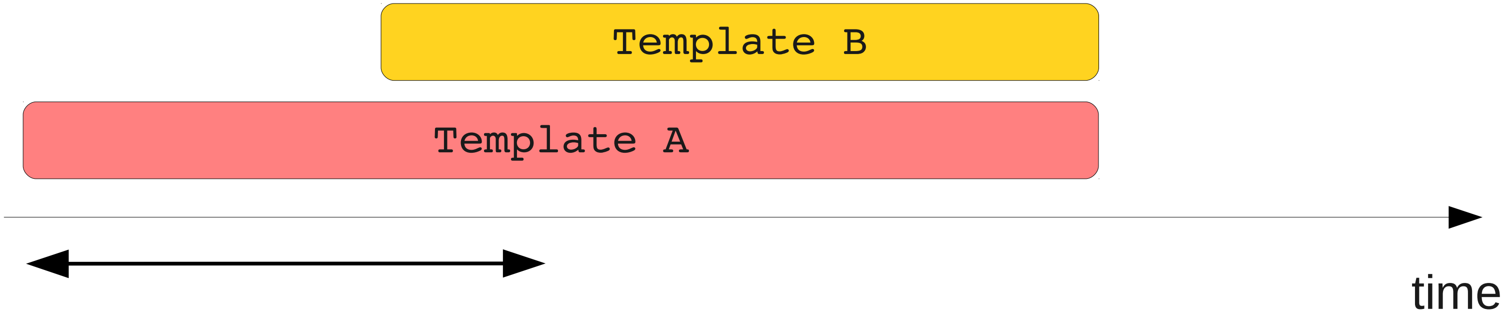
Size *k* of the Training Buffer



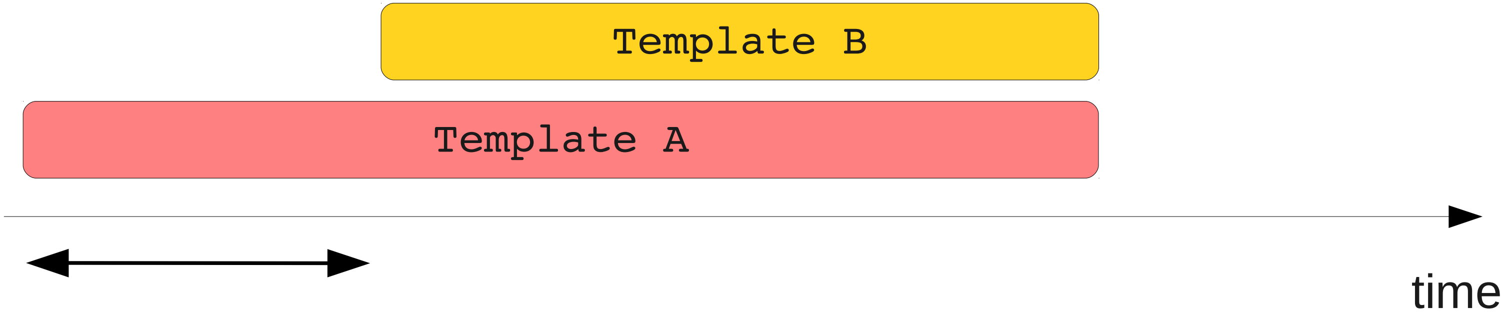
Too small:



Too large:

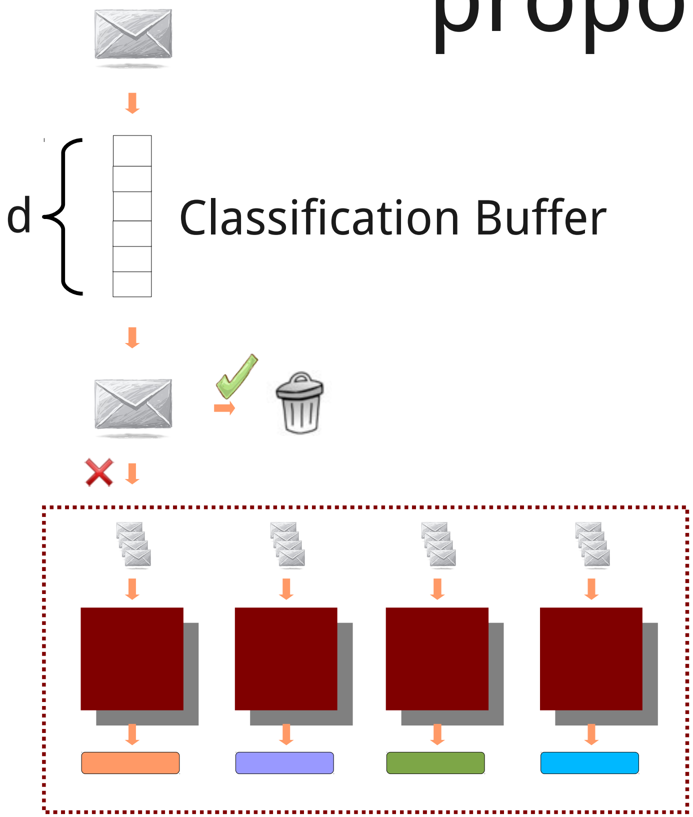


Just right:



Multiple Template Inference - Evaluation

False Negative Rate is inverse proportional to *d*



Interesting Links

- http://www.spamhaus.org/rokso/
- http://www.symanteccloud.com/en/us/globalthreats/
- http://www.commtouch.com/threat-report-january-2012
- http://spamtrackers.eu/wiki/index.php
- http://botlab.org/
- In general: Work by Geoffrey M. Voelker & colleagues: http://cseweb.ucsd.edu/~voelker/

References

- Main Papers used for this presentation:
  - Click Trajectories: End-to-End Analysis of the Spam Value Chain
    K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and Stefan Savage. IEEE Symposium on Security and Privacy, 2011, Oakland, USA.
  - Botnet Judo: Fighting Spam with itself
    A. Pitsillidis, K. Levchenko, C. Kreibich, C. Kanich, G.M. Voelker, V. Paxson, N. Weaver, and S. Savage. Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS Symposiom 2010), San Diego, California. February 2010.
  - Spamalytics: An Empirical Analysis of Spam Marketing Conversion
    C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Proceedings of the 15th ACM Conference on Computer and Communications Security (ACM CCS), Alexandria, Virginia, pp. 3-14. Also appeared in the Communications of the ACM, Vol. 52, No. 9, pp. 99-107, September 2009
- Other sources are mentioned directly on the slides