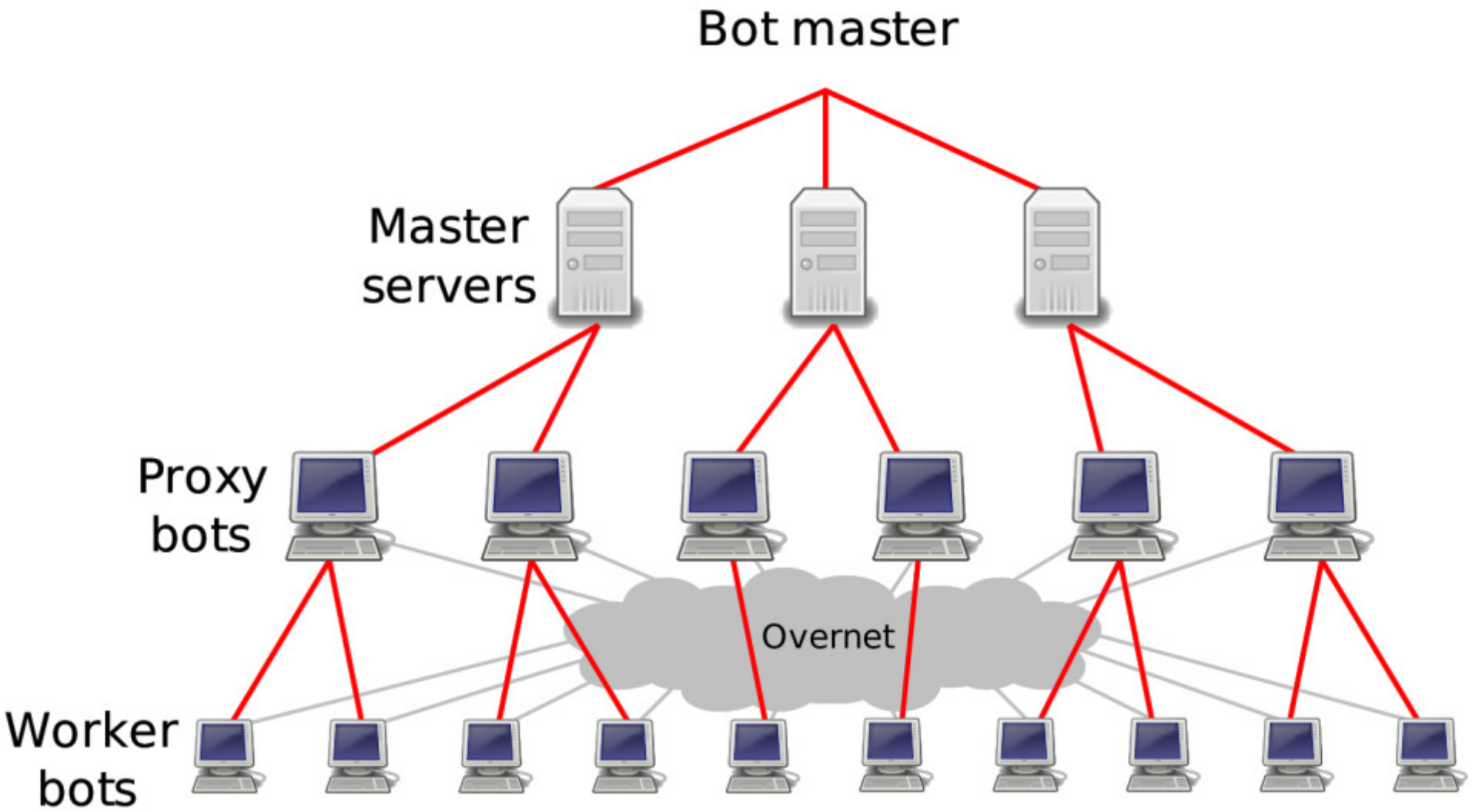
Spamalytics presentation by Ryan

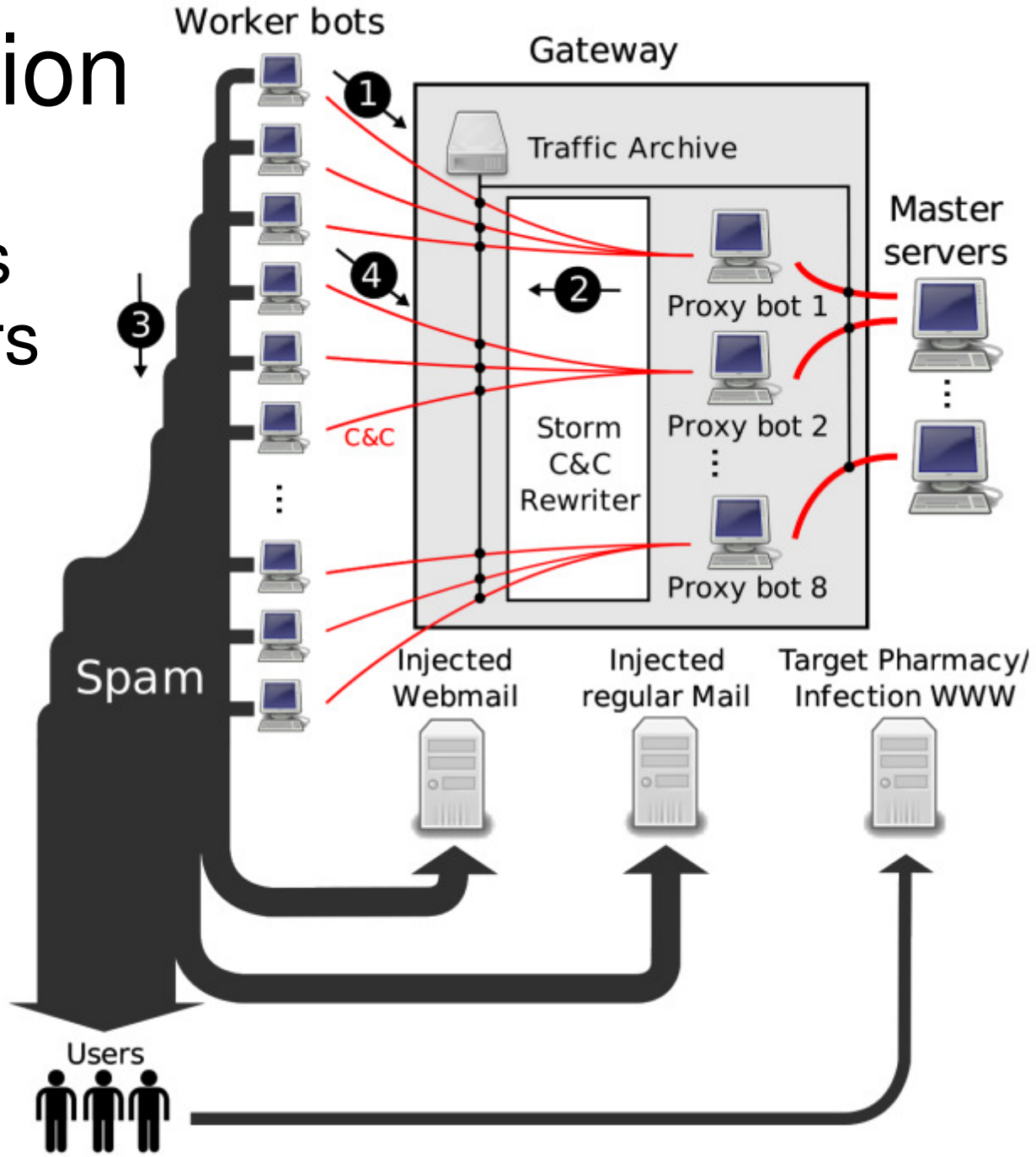
- “An Empirical Analysis of Spam Marketing Conversion”
- By Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage
- International Computer Science Institute, Berkeley, USA
- Dept. of Computer Science and Engineering, University of California, San Diego, USA

Storm Botnet Architecture



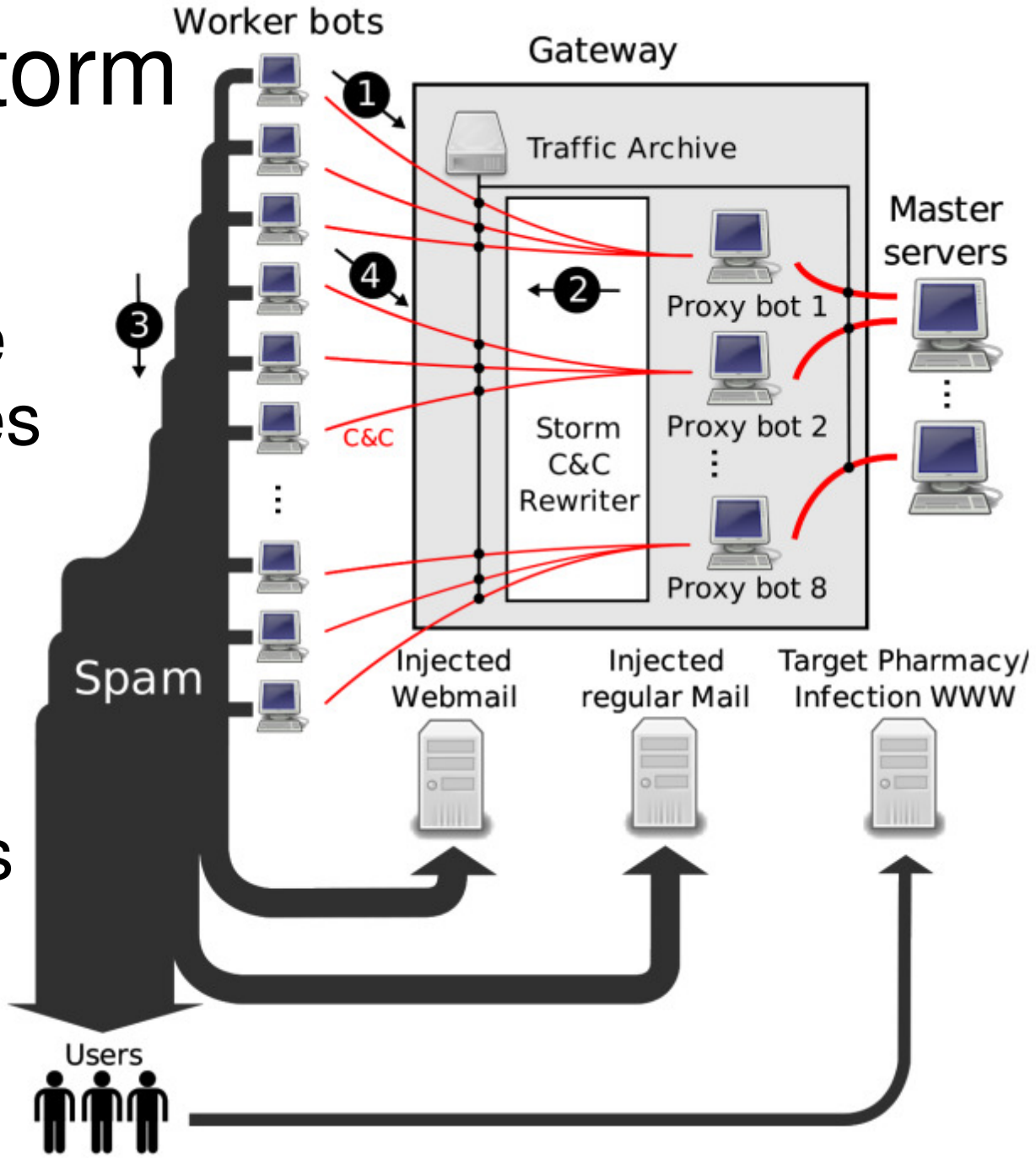
Storm In Action

- Master servers instruct workers via proxy bots
- Workers get templates + addresses from proxies to send spam

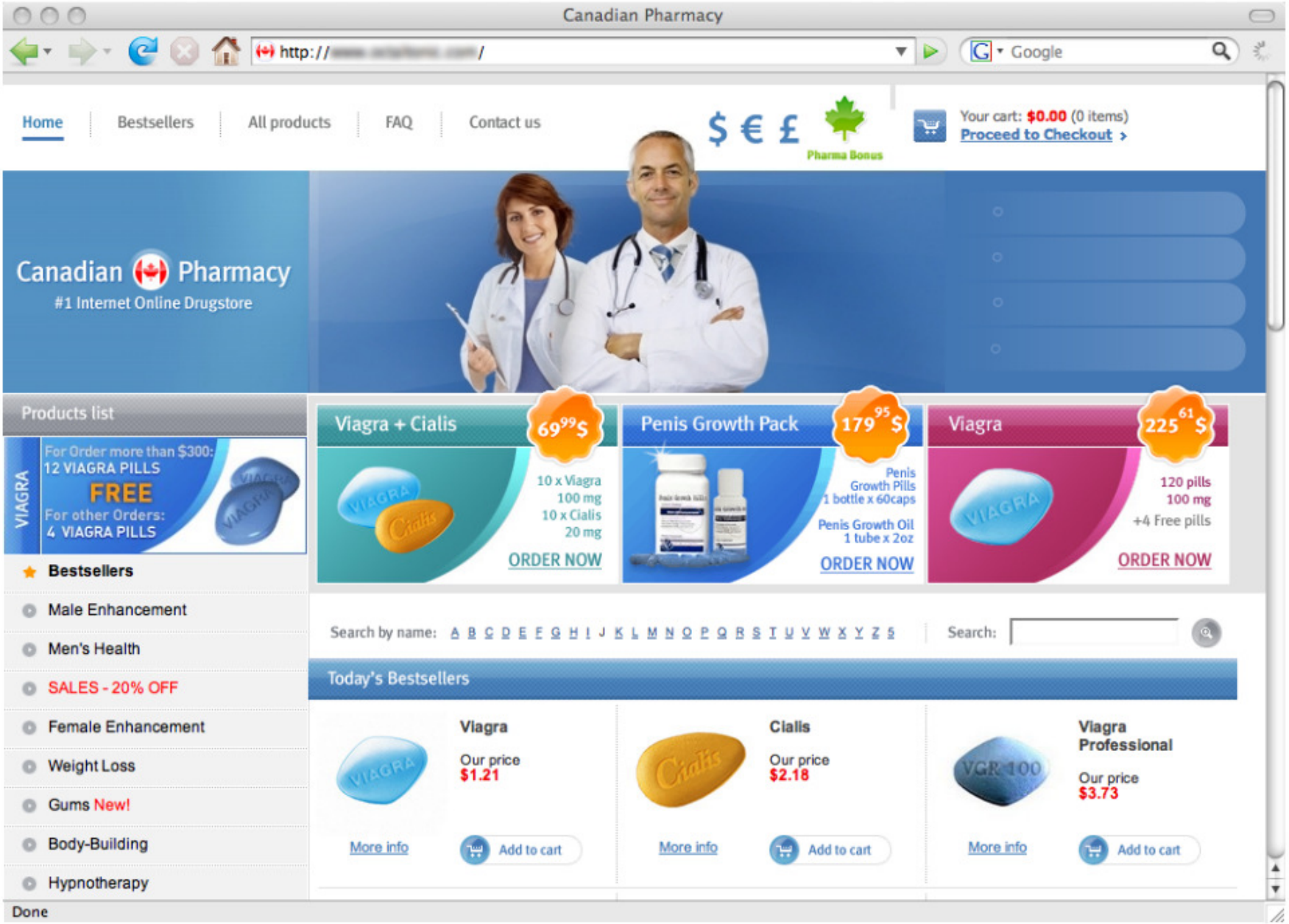


Infiltrating Storm

- Eight proxy servers rewrite spam templates
- Similar spam directs targets to “defanged” researcher-controlled sites



Don't Buy Viagra Here!



Do Not Start This Download

“Defanged” means that the websites look and feel the same but don't actually do anything malicious to the user. For example, the pharmacy site sends a 404 error when the user attempts to check out with items (instead of charging the card).

Results

How much spam do 8 proxies help send out?

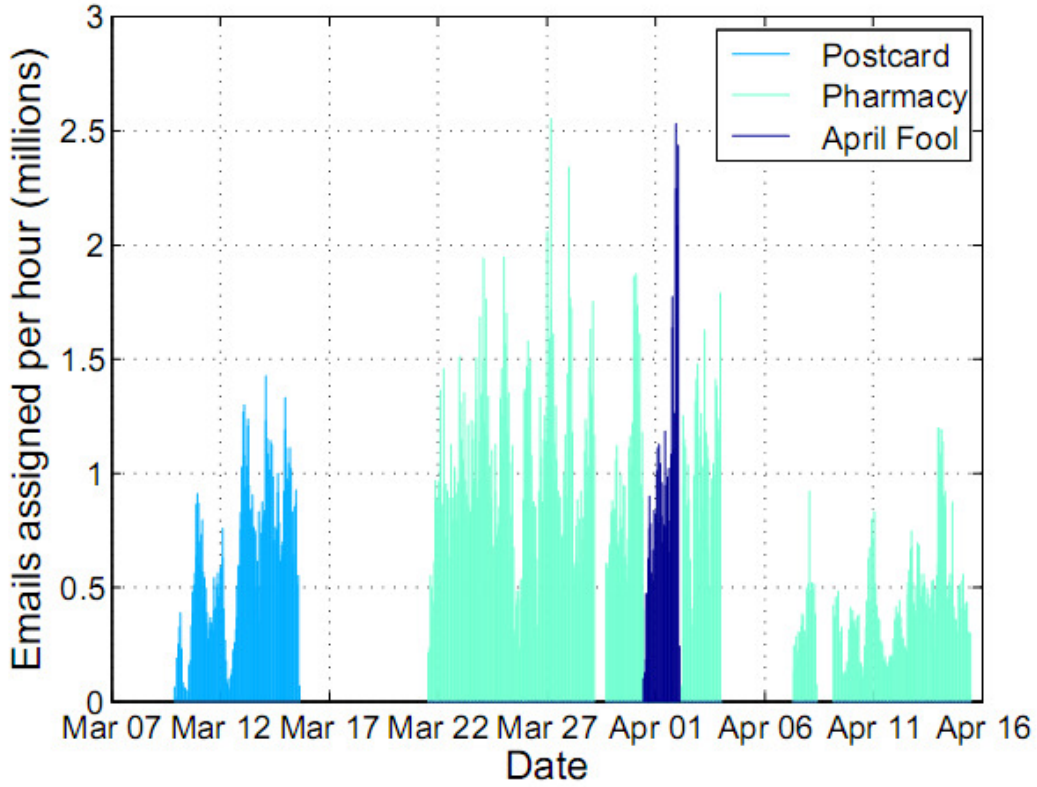


Figure 4: Number of e-mail messages assigned per hour for each campaign.

Results

- Number of Workers connected to proxies

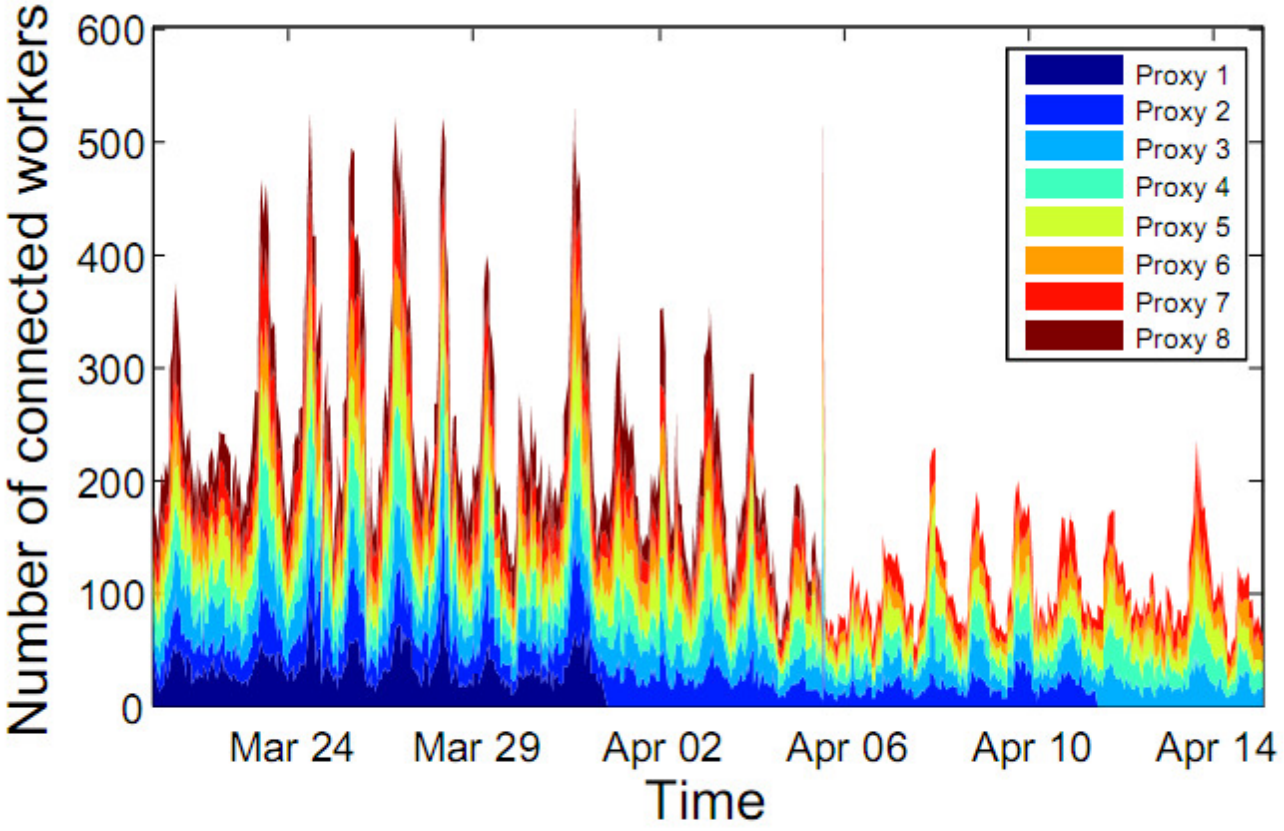


Figure 5: Timeline of proxy bot workload.

Results

- How effective is webmail spam filtering?

Spam Filter	Pharmacy	Postcard	April Fool
Gmail	0.00683%	0.00176%	0.00226%
Yahoo	0.00173%	0.000542%	none
Hotmail	none	none	none
Barracuda	0.131%	N/A	0.00826%

Results

- Who's stupid enough to download/buy?

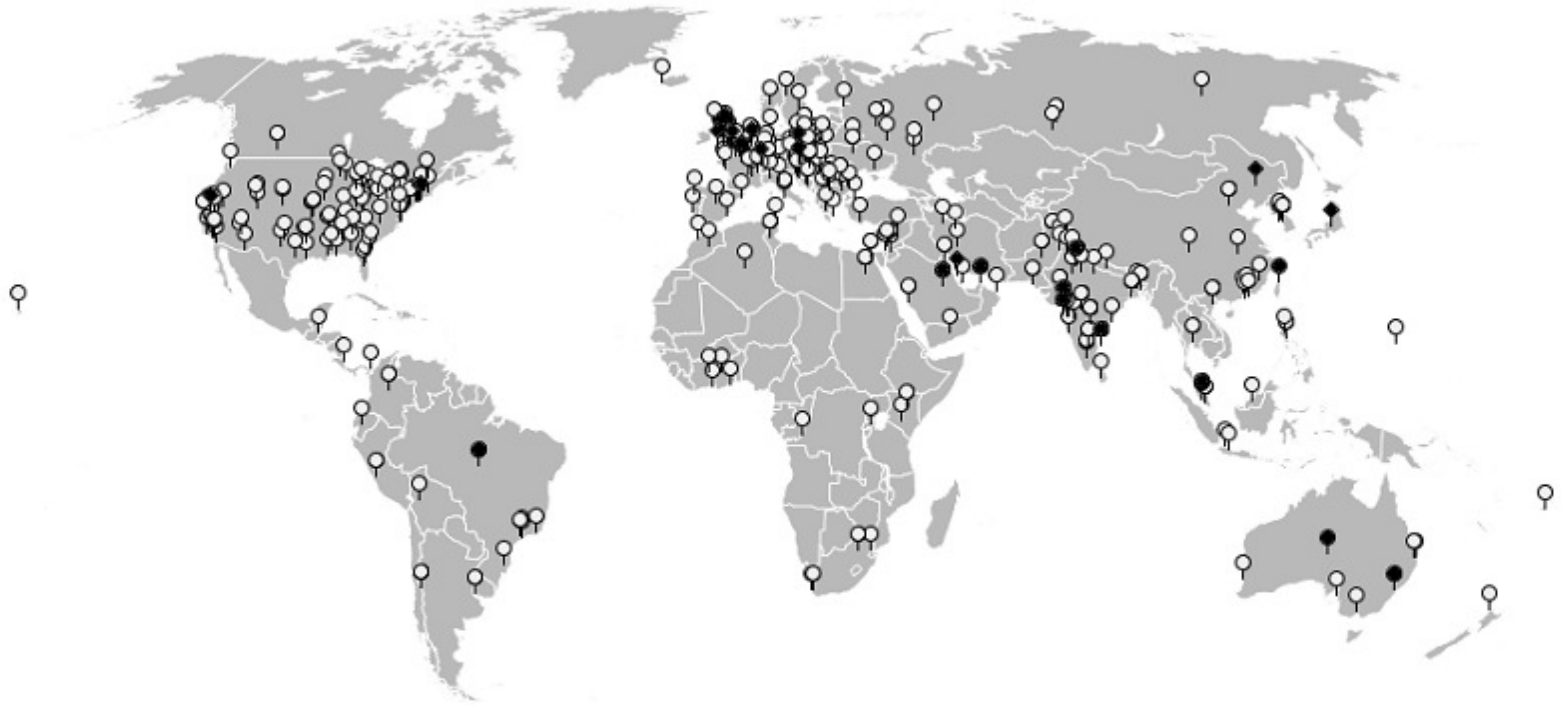


Figure 9: Geographic locations of the hosts that "convert" on spam: the 541 hosts that execute the emulated self-propagation program (light grey), and the 28 hosts that visit the purchase page of the emulated pharmacy site (black).

How much money is it worth?

- A big If: If these results are representative, the Storm Bot Net produced about **$3.5** million in revenue during 2008
- This was likely split between the people behind Storm and with the affiliate web sites where spammed users were sent
- Efforts to fight the spam are significantly impacting the spammer's bottom line

Takeaway

- There is a lot of money in huge-scale spamming
- Nevertheless, better spam-fighting techniques and user education does hurt the spammers
- Spamming techniques and countermeasures will continue to co-evolve
- “Ethical” participation in a bot net is possible?