Released from Prison, Spammer Who Stole 17.5 Million Passwords Apologizes and Reforms (zdnet.com)

14

Posted by EditorDavid on Sunday September 15, 2019 @07:34AM from the new-leaf dept.

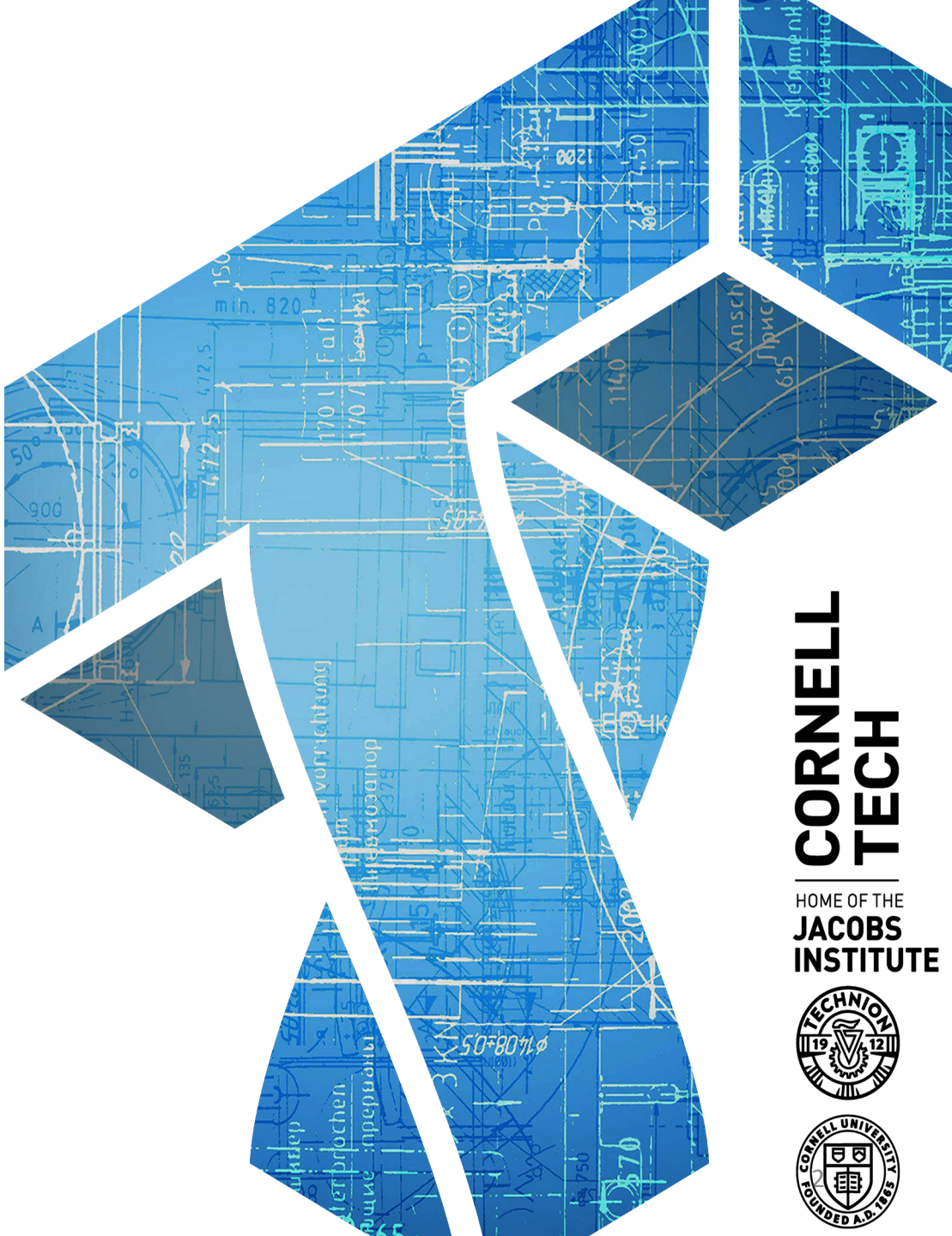
An anonymous reader quotes ZDNet:

> Kyle Milliken, a 29-year-old Arkansas man, was released last week from a federal work camp. He served 17 months for hacking into the servers of several companies and stealing their user databases. Some of the victims included Disqus, from where he stole 17.5 million user records, Kickstarter, from where he took 5.2 million records, and Imgur, with 1.7 million records. For years, Milliken and his partners operated by using the credentials stolen from other companies to break into more lucrative accounts on other services.
>
> If users had reused their passwords, Milliken would access their email inboxes, Facebook, Twitter, or Myspace accounts, and post spam promoting various products and services. From 2010 to 2014, Milliken and his colleagues operated a successful spam campaign using this simple scheme, making more than $1.4 million in profits, and living the high life. Authorities eventually caught up with the hacker. He was arrested in 2014, and collaborated with authorities for the next years, until last year, when it leaked that he was collaborating with authorities and was blackballed on the cybercrime underground....
>
> In an interview with ZDNet last week, Milliken said he's planning to go back to school and then start a career in cyber-security... [H]e publicly apologized to the Kickstarter CEO on Twitter. "I've had a lot of time to reflect and see things from a different perspective," Milliken told ZDNet. "When you're hacking or have an objective to dump a database, you don't think about who's on the other end. There's a lot of talented people, a ton of work, and even more money that goes into creating a company... there's a bit of remorse for putting these people through cyber hell."

CS 5435: Commercially-motivated abuse

Instructor: Tom Ristenpart

https://github.com/tomrist/cs5435-fall2019

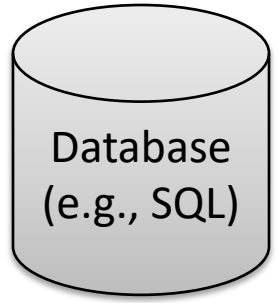


CORNELL TECH

HOME OF THE JACOBS INSTITUTE

Airbnb as an example service

Hosts



Guests

Last time: Authentication and account break-in

Today: abusing services with (authenticated) access to them

Email spam and scams

- Spam
  - unsolicited bulk emails
  - Illegal in USA since CAN-SPAM act of 2003
- Scams
  - Nigerian emails (advanced fee fraud / confidence trick)
- Phishing
  - trick users into downloading malware, submitting password to attacker, CC info to attacker, etc.
  - Spear phishing: targeted on individuals (used in high-profile intrusions)

Jon

Junk - Exchange August 24, 2019 at 3:16 PM

J

Official request

Reply-To: jocun01250@mail2banker.com

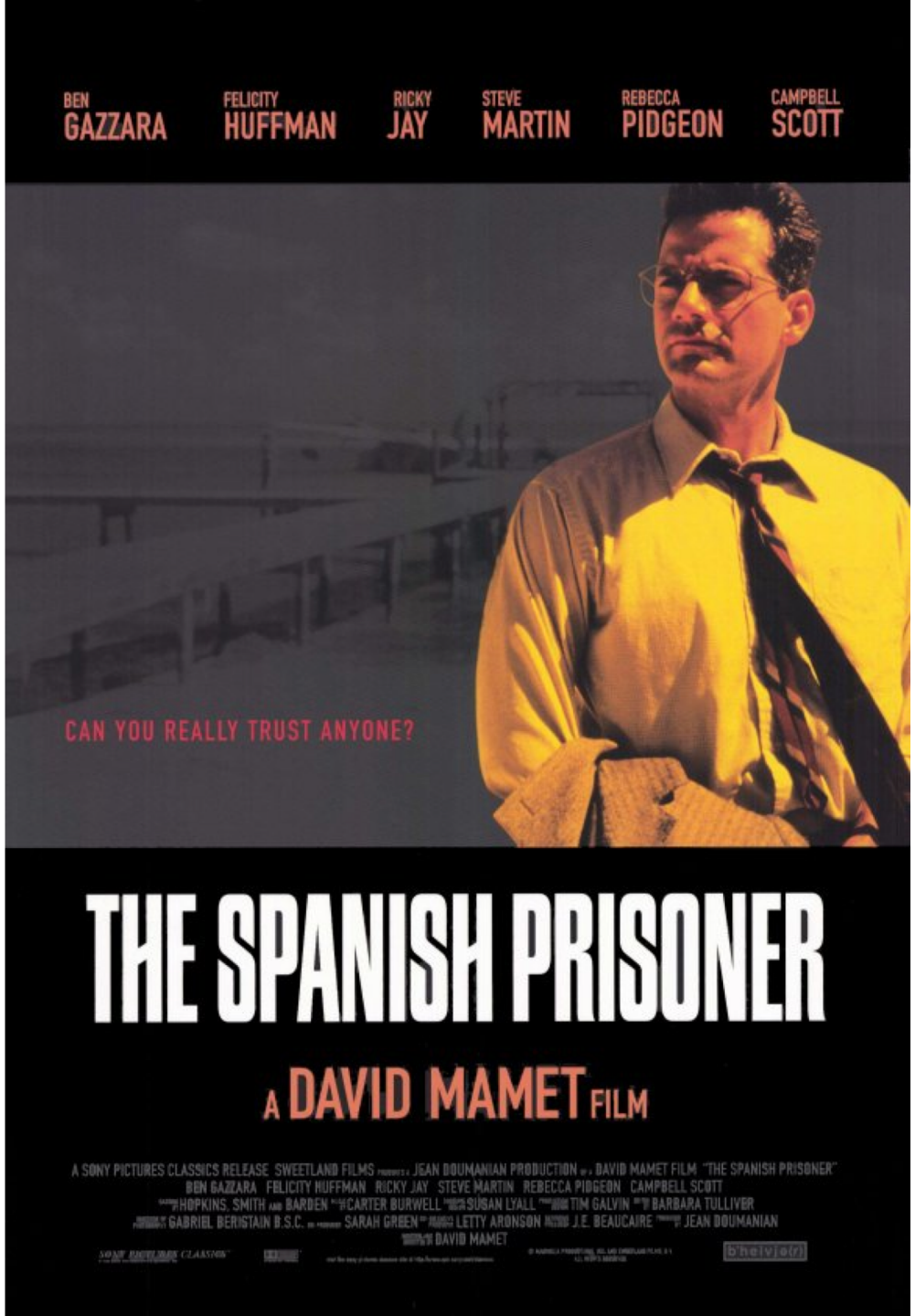
Hello,

This is an official request to you, we have a deceased client whose inheritance we wish to payout to avoid seizure. We are no longer paying for private searches to trace his relatives after today. We contacted you knowing you could be. Please treat urgent.

Regards,
Jon

Spanish Prisoner confidence trick

- 19th century
- In contact with rich guy in Spanish prison
- Just need a little money to bribe guards, he'll reward you greatly
- ***Advance-fee scam***



2018 CRIME TYPES

By Victim Count

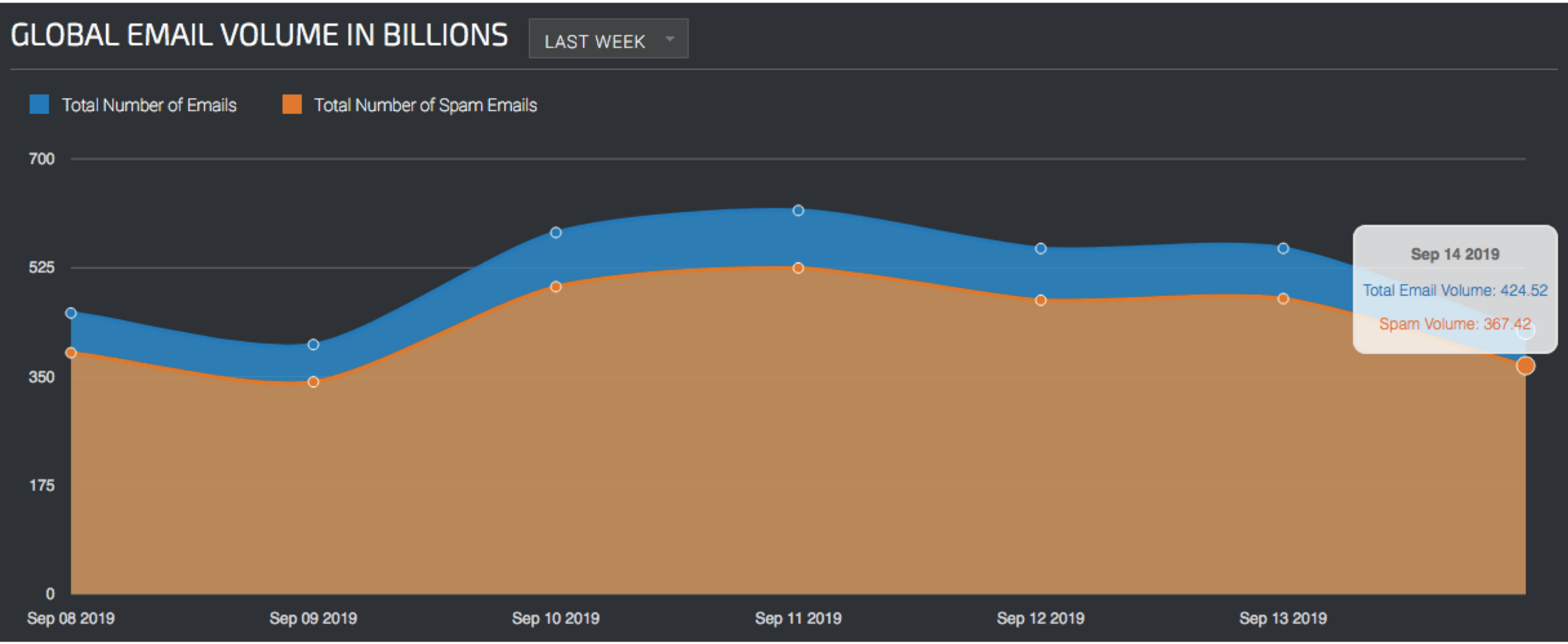
Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,936	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,480
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

https://pdf.ic3.gov/2018_IC3Report.pdf

By Victim Loss

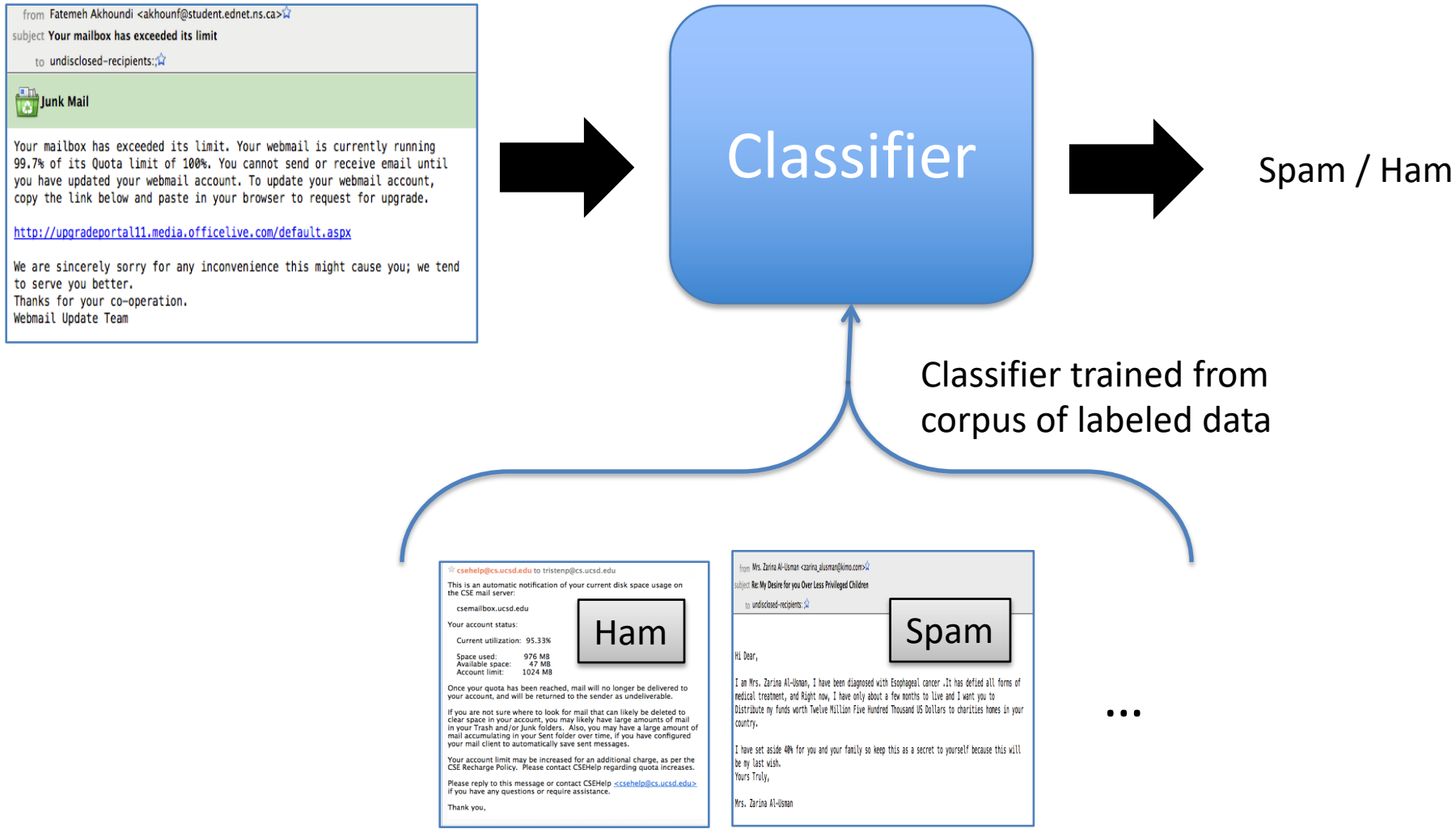
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,297,803,489	Tech Support	$38,697,026
Confidence Fraud/Romance	$362,500,761	Harassment/Threats of Violence	$21,903,829
Investment	$252,955,320	Misrepresentation	$20,000,713
Non-Payment/Non-Delivery	$183,826,809	IPR/Copyright and Counterfeit	$15,802,011
Real Estate/Rental	$149,458,114	Civil Matter	$15,172,692
Personal Data Breach	$148,892,403	Malware/Scareware/ Virus	$7,411,651
Corporate Data Breach	$117,711,989	Health Care Related	$4,474,792
Identity Theft	$100,429,691	Ransomware	*$3,621,857
Advanced Fee	$92,271,682	Denial of Service/TDos	$2,052,340
Credit Card Fraud	$88,991,436	Re-Shipping	$1,684,179
Extortion	$83,357,901	Charity	$1,006,379
Spoofing	$70,000,248	Gambling	$926,953
Government Impersonation	$64,211,765	Crimes Against Children	$265,996
Other	$63,126,929	Hacktivist	$77,612
Lottery/Sweepstakes	$60,214,814	Terrorism	$10,193
Overpayment	$53,225,507	No Lead Value	$0.00
Phishing/Vishing/Smishing/Pharming	$48,241,748		
Employment	$45,487,120		

https://pdf.ic3.gov/2018_IC3Report.pdf

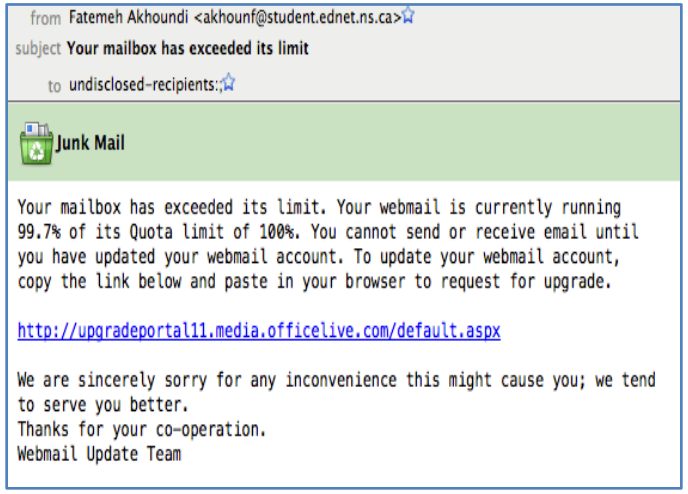


https://www.talosintelligence.com/reputation_center/email_rep#tab=1

Spam Classifiers



Naïve Bayes Classifier


from Fatemeh Akhoundi <akhounf@student.ednet.ns.ca>
subject **Your mailbox has exceeded its limit**
to undisclosed-recipients:;

Junk Mail

Your mailbox has exceeded its limit. Your webmail is currently running 99.7% of its Quota limit of 100%. You cannot send or receive email until you have updated your webmail account. To update your webmail account, copy the link below and paste in your browser to request for upgrade.

http://upgradeportal11.media.officelive.com/default.aspx

We are sincerely sorry for any inconvenience this might cause you; we tend to serve you better.
Thanks for your co-operation.
Webmail Update Team

Represent email as "bag of words"

quota	1	x_1
webmail	4	x_2
cornell	0	x_3
fee	1	x_4
⋮	⋮	

Intuition: spam and ham have different distribution of keywords

$$\Pr[\text{spam} \mid x_1, x_2, \ldots, x_n] = \frac{\Pr[x_1, x_2, \ldots, x_n \mid \text{spam}]\ \Pr[\text{spam}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

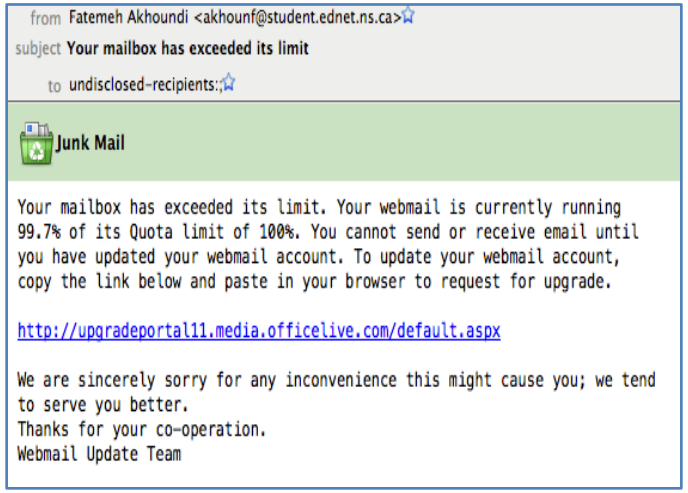
Bayes' theorem

$$= \frac{\Pr[\text{spam}] \prod \Pr[x_i \mid \text{spam}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

"Naïve": assume words independent

$$\Pr[\text{ham} \mid x_1, x_2, \ldots, x_n] = \frac{\Pr[\text{ham}] \prod \Pr[x_i \mid \text{ham}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

Naïve Bayes Classifier



Represent email as "bag of words"

quota	1	x_1
webmail	4	x_2
cornell	0	x_3
fee	1	x_4
⋮	⋮	

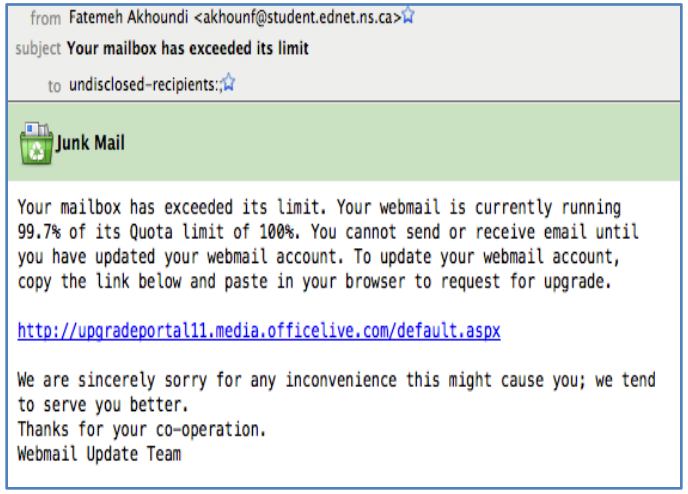
Intuition: spam and ham have different distribution of keywords

$$\Pr[\text{spam} \mid x_1, x_2, \ldots, x_n] = \frac{\Pr[\text{spam}] \prod \Pr[x_i \mid \text{spam}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

$$\Pr[\text{ham} \mid x_1, x_2, \ldots, x_n] = \frac{\Pr[\text{ham}] \prod \Pr[x_i \mid \text{ham}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

Classify as spam if: $\Pr[\text{spam} \mid x_1, x_2, \ldots, x_n] > \Pr[\text{ham} \mid x_1, x_2, \ldots, x_n]$

Naïve Bayes Classifier


from Fatemeh Akhoundi <akhounf@student.ednet.ns.ca>
subject **Your mailbox has exceeded its limit**
to undisclosed-recipients:;

Junk Mail

Your mailbox has exceeded its limit. Your webmail is currently running 99.7% of its Quota limit of 100%. You cannot send or receive email until you have updated your webmail account. To update your webmail account, copy the link below and paste in your browser to request for upgrade.

http://upgradeportal11.media.officelive.com/default.aspx

We are sincerely sorry for any inconvenience this might cause you; we tend to serve you better.
Thanks for your co-operation.
Webmail Update Team

Represent email as "bag of words"

quota	1	x_1
webmail	4	x_2
cornell	0	x_3
fee	1	x_4
⋮	⋮	

Intuition: spam and ham have different distribution of keywords

Estimate these from labeled training data

$$\Pr[\text{spam} \mid x_1, x_2, \ldots, x_n] = \frac{\Pr[\text{spam}] \prod \Pr[x_i \mid \text{spam}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

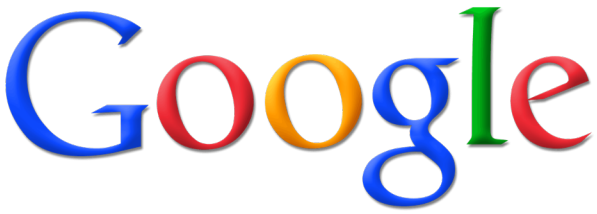
$$\Pr[\text{ham} \mid x_1, x_2, \ldots, x_n] = \frac{\Pr[\text{ham}] \prod \Pr[x_i \mid \text{ham}]}{\Pr[x_1, x_2, \ldots, x_n]}$$

Classify as spam if: $\Pr[\text{spam}] \prod \Pr[x_i \mid \text{spam}] > \Pr[\text{ham}] \prod \Pr[x_i \mid \text{ham}]$

Spam classifiers

- Nowadays classifiers more complex than this
  - Other features: Who is sender? How many links embedded?
  - Can update in real-time given labeling by user
  - For larger orgs, can leverage wide view across many email recipients (Gmail)
- Nowadays some companies do pretty good job of making sure spam doesn't hit your inbox
  - 95% of email gets filtered as spam (2009, ENISA Spam Survey)

Web services in-class exercise



In-class 5-minute exercise:

Discuss your favorite web service:

1. What commercially-motivated abuse might it have to contend with?
2. How might you prevent it?

Removing bad actors from services is *hard*

- **Facebook**: spammer accounts, fake fraud accounts, …
- **Twitter**: illicit promotional accounts, …
- **Yelp:** fake reviews, fake restaurants, …
- **AirBNB**: scam rental or experience ads
- **Lyft**: colluding drivers + riders
- **Google**: spammers using Gmail, advertisers violating terms of service, SEO, Play store bad apps, …

The Flourishing Business of Fake YouTube Views

Plays can be bought for pennies and delivered in bulk, inflating videos' popularity and making the social media giant vulnerable to manipulation.

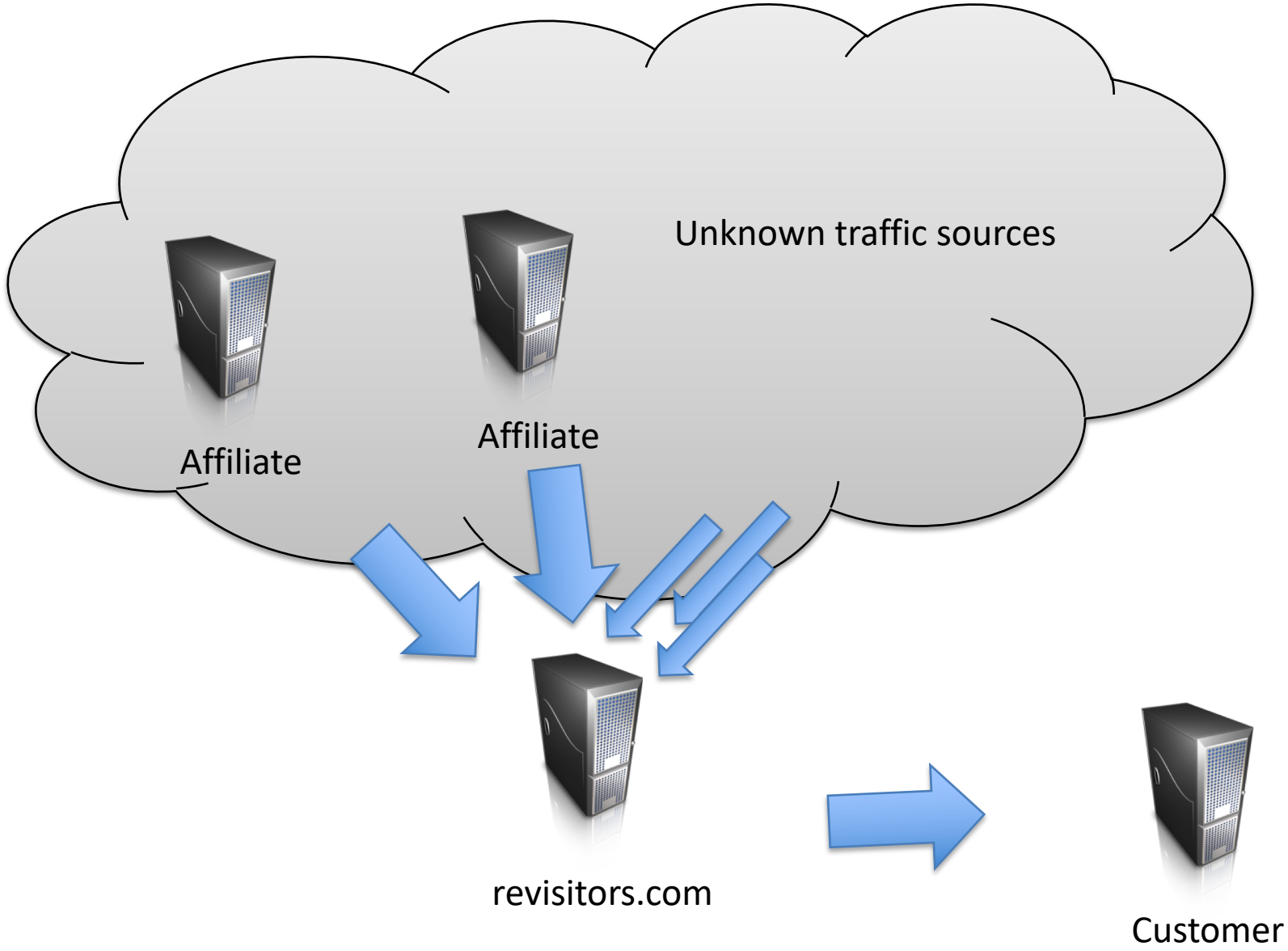
By MICHAEL H. KELLER AUG. 11, 2018

https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html

"At one point in 2013, YouTube had as much traffic from bots masquerading as people as it did from real human visitors, according to the company."

Traffic sellers

- Click fraud
- Click traffic sellers
  - grey-market


Unknown traffic sources
Affiliate
Affiliate
revisitors.com
Customer

Traffic sellers (circa 2008)

Quality of website's English ↓

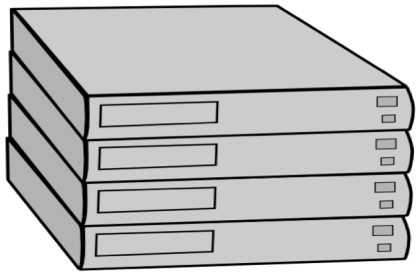
Web site	CP10k	Claimed traffic source
www.trafficdeliver.com	~$34.69	"Advertiser exchange"
revisitors.com	~$48.95	Recently expired domain redirection?
qualitytrafficsupply.com	~$55.00	Contextual advertisements
mediatraffic.com	~$70	AdWare (Voomba) pop-ups

Targeted vs. untargeted: specify geographic preferences

Affiliate networks: paid to send traffic

Traffic resellers: resell purchased traffic

Experimental methodology



(1) Setup several web sites (xxx.sysnet.ucsd.edu)

2 pages: index.html is landing site
lucky.html linked to by index.html

Website instrumented to log all traffic, client-side javascript to measure user interaction

(2) Attempt to purchase web traffic

Used temporary VISA number, but real name, etc.

(3) Sit back and let the research data come to us ...

Adventures in purchasing web traffic...

Giving people money not as easy as I expected:

RE: Refund - [2423-DLXC-4301] [82a2e44b]

2Checkout Help Desk ========= Please enter your reply ABOVE above this line ========= Hello Tom, ... Dec 6 (5 days ago)

2Checkout Help Desk A staff member has replied to your question: Seasons Greetings Tom, Thank you... Dec 6 (5 days ago)

2Checkout Help Desk Thank you for adding a message to your question. We will respond to your mess... Dec 6 (4 days ago)

2Checkout Help Desk to me show details Dec 6 (4 days ago) Reply

========= Please enter your reply ABOVE above this line =========

Hello Tom,

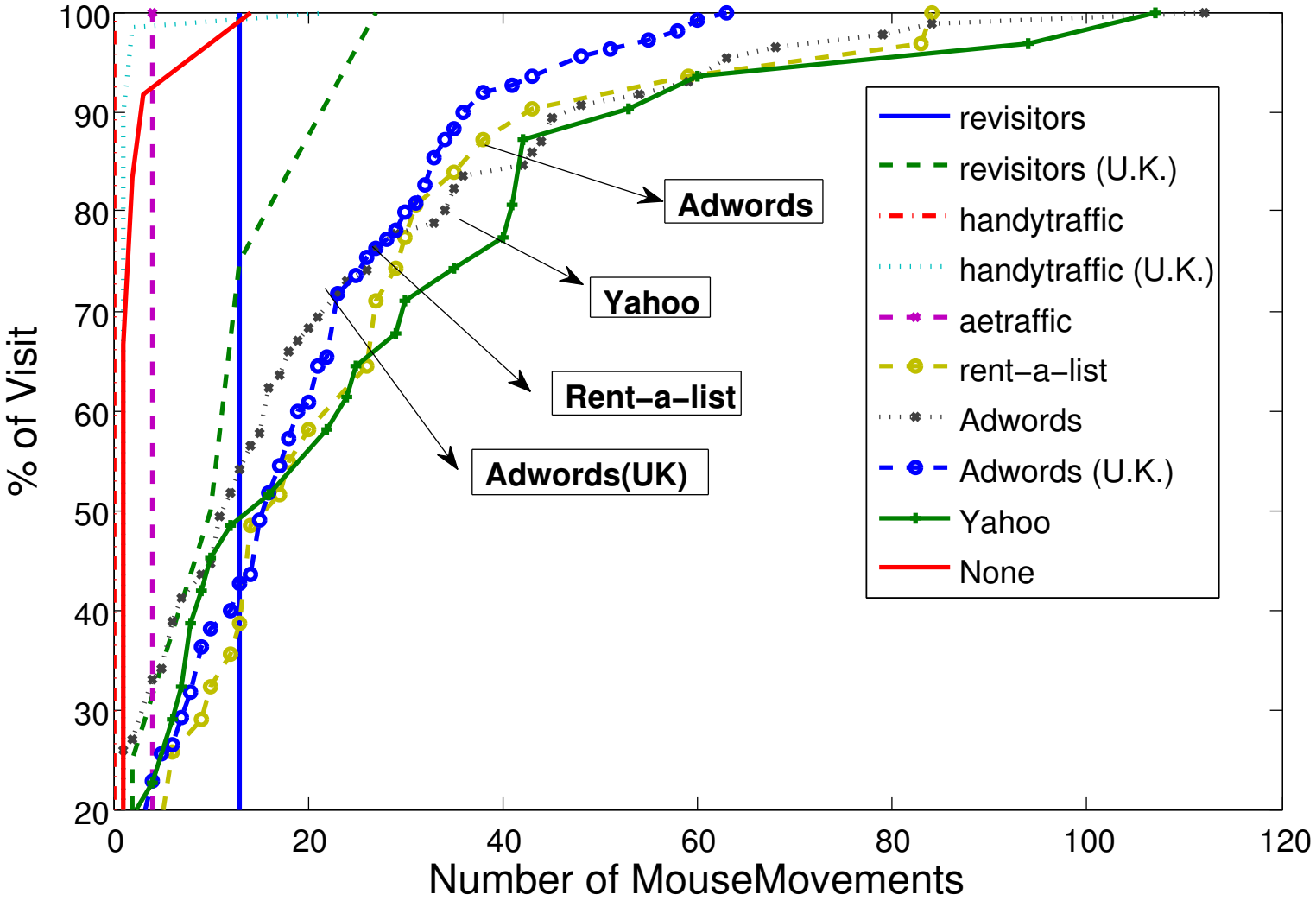
A staff member has replied to your question:

Dear Tom,

Thank you for contacting 2Checkout.com. I apologize for the delay in responding to your inquiry. The order was actually canceled trafficdeliver.com. They believe the order to be fraudulent. I have forwarded your inquiry to trafficdeliver.com. They will be contacting you via e-mail shortly. If you do not receive a response in a timely manner, please feel free to reopen this ticket for additional assistance.

Looking to make your holidays happier? 2Checkout makes it easy! Simply visit your favorite search engine and type in 2Checkout + and the type of merchandise you are looking for. It's the easy way to enjoy a fast, safe shopping experience online.

Thank You,
Josh Karamian
Customer Care
2Checkout.com
http://www.2Checkout.com



(b) CDF of # of mouse moves per visit across all visits

Zhang et al., Got Traffic? An Evaluation of Click Traffic Providers, 2011

How to prevent fraudulent actions?

- **Content analysis**
  - Spam filters
- **Identify bad accounts**
  - Correlate bad actions with accounts, try to detect bots
  - Sock-puppet accounts (many controlled by one person)
- **Identify bad devices**
  - Device cookies to correlate different account accesses
  - IP blacklists, ISP blacklists
- **Target fraud-support infrastructure**
  - Botnet takedowns, bank accounts, jail sentences

Botnets

- Botnets:
  - Command and Control (C&C)
  - Zombie hosts (bots)
- C&C type:
  - centralized, peer-to-peer
- Infection vector:
  - spam, random/targeted scanning
- Usage:
  - What they do: spam, DDoS, SEO, traffic generation, …

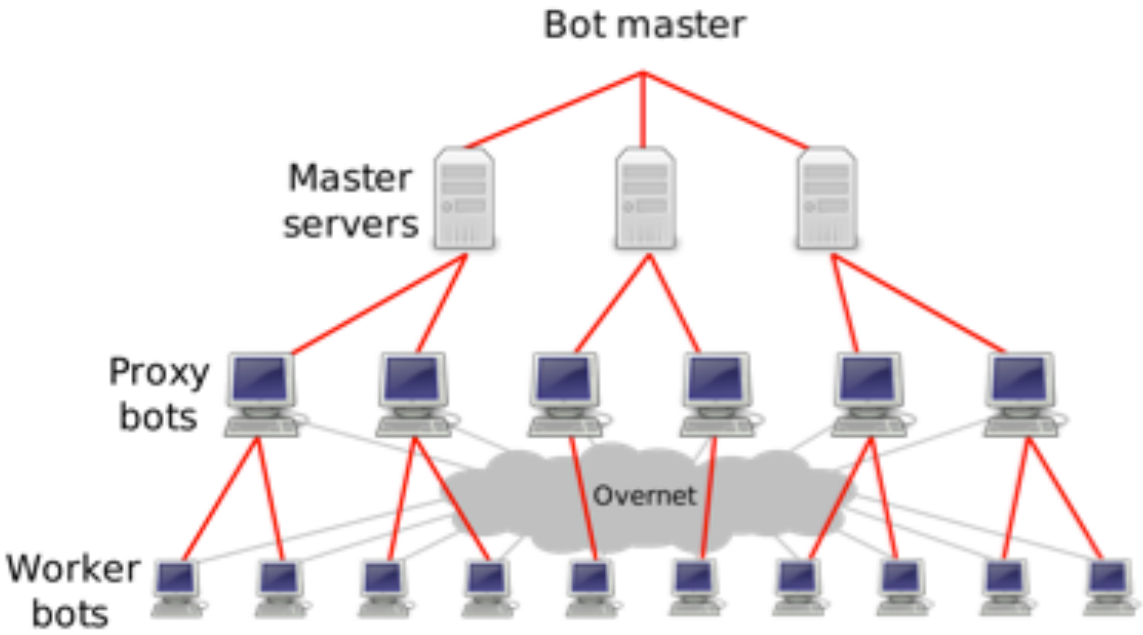


Figure 1: The Storm botnet hierarchy.

Storm botnet (2007-08)

- September 2007
  - Media: 1 – 50 million bots
  - More likely: 10,000s to 100,000s
- Early spam campaigns used titles such as "230 dead as storm batters Europe."
- Propagated via spam linking to malware
- Thought to be controlled by Russian Business Network

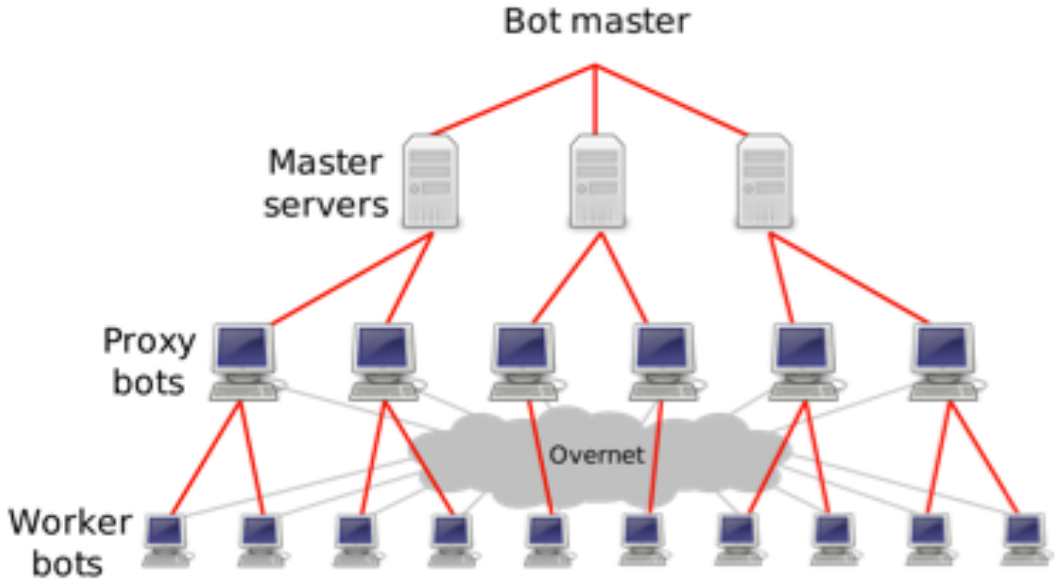


Figure 1: The Storm botnet hierarchy.

Features:

- Uses P2P (Overnet/Kademlia)
- Uses fast-flux DNS for hosting on named sites
- Binary has gone through many revisions
- Features of P2P network have evolved with time
- Hides on machine with rootkit technology

[Enright 2007]

See also: http://cseweb.ucsd.edu/~savage/papers/login08.pdf

How to make money off a botnet?

- Rental
  - "Pay me money, and I'll let you use my botnet… no questions asked"
- DDoS extortion / DDoS for hire
  - "Pay me or I take your legitimate business off web"
  - "Pay me and I'll take someone else off Internet"
- Bulk traffic selling
  - "Pay me to direct bots to websites to boost visit counts"
- Click fraud, SEO
  - "Simulate clicks on advertised links to generate revenue"
  - Cloaking, link farms, etc.
- Theft of monetizable data (eg., financial accounts)
- Data ransom (now called ransomware)
  - "I've encrypted your harddrive, now pay me money to unencrypt it"
- Spam to advertise products

Underground forums

Category	Threads B	Threads S	Users B	Users S	Top Subcategory
payments	8,507	8,092	1,539	1,409	paysafecard
game-related	2,379	2,584	924	987	steam
accounts	2,119	2,067	850	974	rapidshare
credit cards	996	1160	467	566	unspecified cc
software/keys	729	1410	422	740	key/serial
fraud tools	652	1155	363	601	socks
tutorials/guides	950	537	562	393	tutorials
mail/drop srvs	751	681	407	364	packstation
merchandise	493	721	264	404	ipod
services	266	916	176	555	carder

Table 6: Top 10 most commonly traded merchandise categories on LC.

[Motoyama et al., An Analysis of Underground Forums, 2011]

How to make money off financial credentials?

- Money mules
  - Deposits into mules' account from the victim's
  - Mule purchases items using stolen CCN, sells them online
  - Mule withdraws cash from ATMs using victim credentials
- Wires money to (for example) former Soviet Union

from Richard Hill <hill@hetajobs.com>

subject **Cool Student Job**

to pubs@cs.wisc.edu

reply

Dear Student,

I would like to offer you a new interesting and respectable job!
We are looking for people to work as professional distance-based typists. No experience is needed!
If you're eager to use your skills to make some additional cash, then you might want to consider a home typing position!

All data entry operators work from home and are independent contractors.
You typically set your own hours and work from home on projects that are enjoyable!
Average monthly earnings start from $1000 to $3000 or more.

Requirements:
-Computer with Internet access.
-Good Typing Skills.
-Basic Internet knowledge.
-Basic Computer and Typing Skills.

You will not have to devote full time hours. These assignments can be done on your time.
They may be done in Internet cafes or where ever you can get Internet access!
If you are interested just reply to my email!

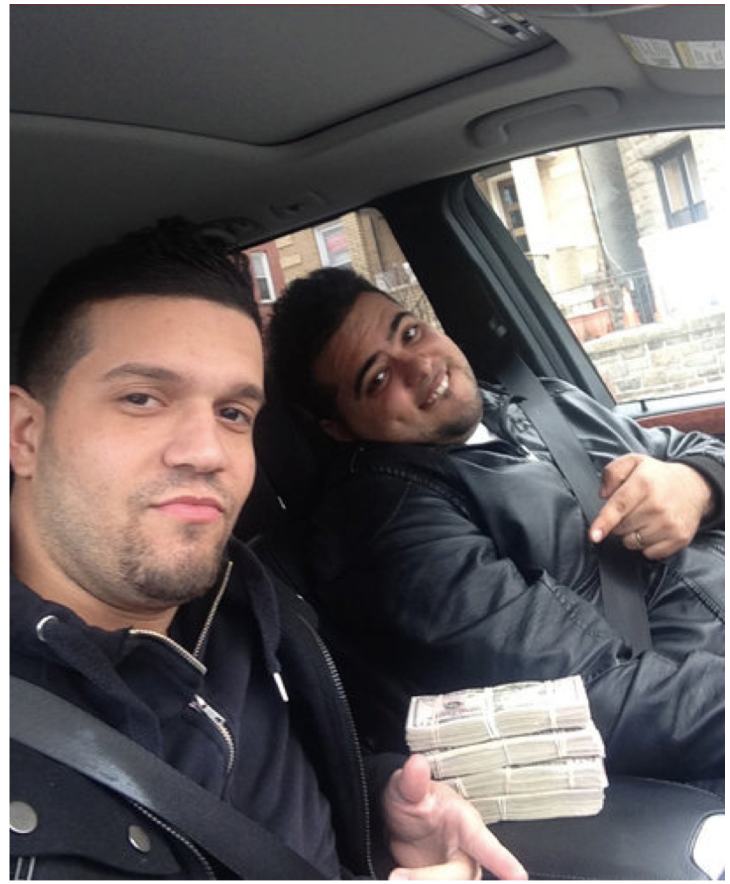
Best Regards,

Richard Hill
Local Recruitment Manager

06 Crooks Net Millions in Coordinated ATM Heists

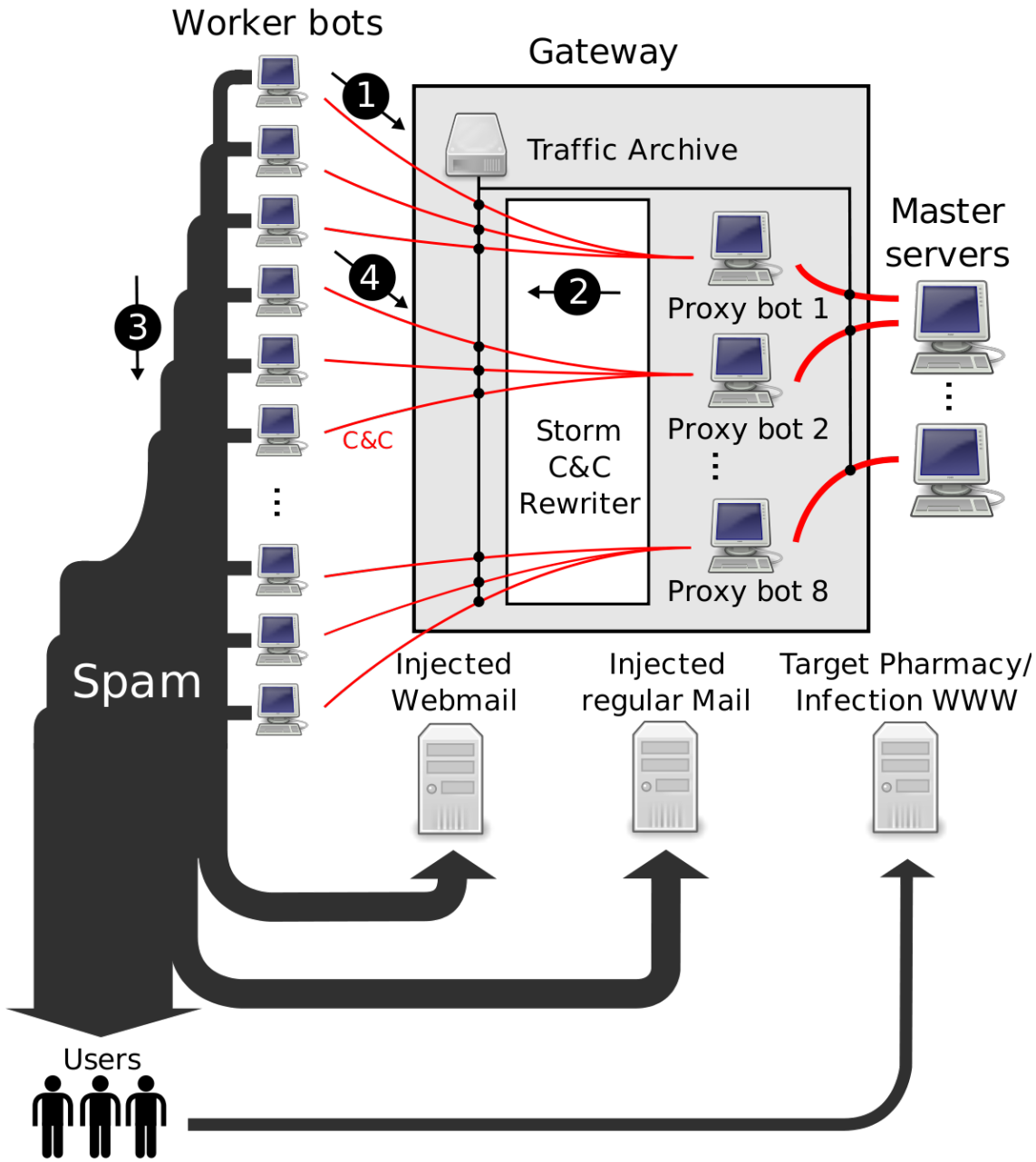
FEB 13

Organized cyber criminals stole almost $11 million in two highly coordinated ATM heists in the final days of 2012, KrebsOnSecurity has learned. The events prompted **Visa** to warn U.S. payment card issuers to be on high-alert for additional ATM cash-out fraud schemes in the New Year.



Botnet takeover studies

- Spamalytics [Kanich et al., 2008]
  - Storm botnet
  - Rewrote spam to redirect to researcher-controlled websites
  - **Goal**: click-through rate measurement



Kanich et al., Spamalytics: An Empirical Analysis of Spam Marketing Conversion, 2008

The victims

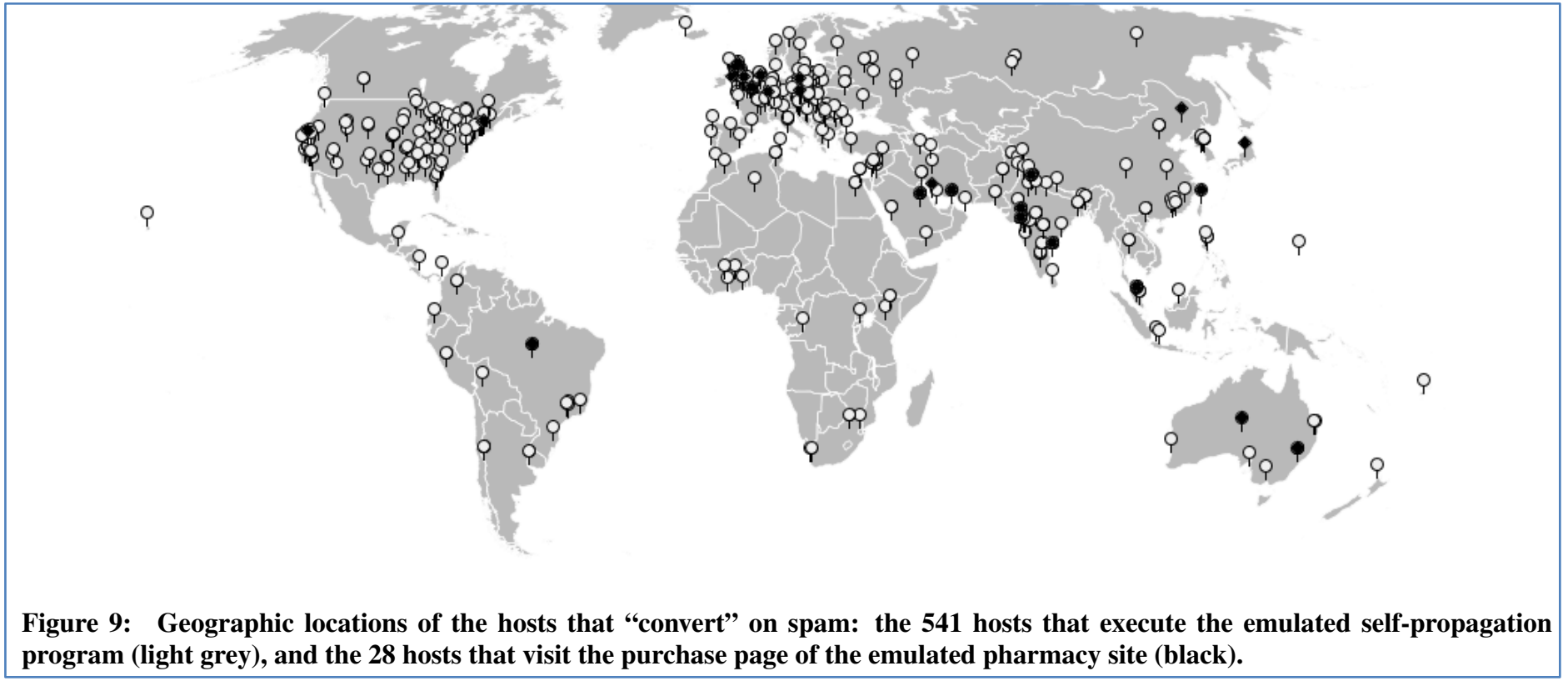


Figure 9: Geographic locations of the hosts that "convert" on spam: the 541 hosts that execute the emulated self-propagation program (light grey), and the 28 hosts that visit the purchase page of the emulated pharmacy site (black).

Kanich et al., Spamalytics: An Empirical Analysis of Spam Marketing Conversion, 2008

Observed Conversion Rate

- 350 million email messages delivered
- 26 day campaign
- 28 “sales”
  - 0.00001%
  - 27 of these male-enhancement products

Botnet countermeasures?

- Infection prevention
- Infection detection
- C&C take-down
- Undermine the economics
  - Banking take-down

C&C takedowns

Microsoft Seizes ZeuS Servers in Anti-Botnet Rampage

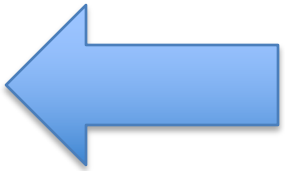
BY KIM ZETTER 03.26.12 2:45 PM

It's not the first time Microsoft has attempted to take down botnets. The company previously attacked three other botnets — Waledac, Rustock and Kelihos — through similar civil suits that allowed the company to seize web addresses and associated computers. The gains from such takedowns, however, are generally short-lived. After Waledac was targeted, the criminals behind it simply altered their software to thwart easy detection and launched a new botnet.

http://www.wired.com/threatlevel/2012/03/microsoft-botnet-takedown/

Botnet countermeasures?

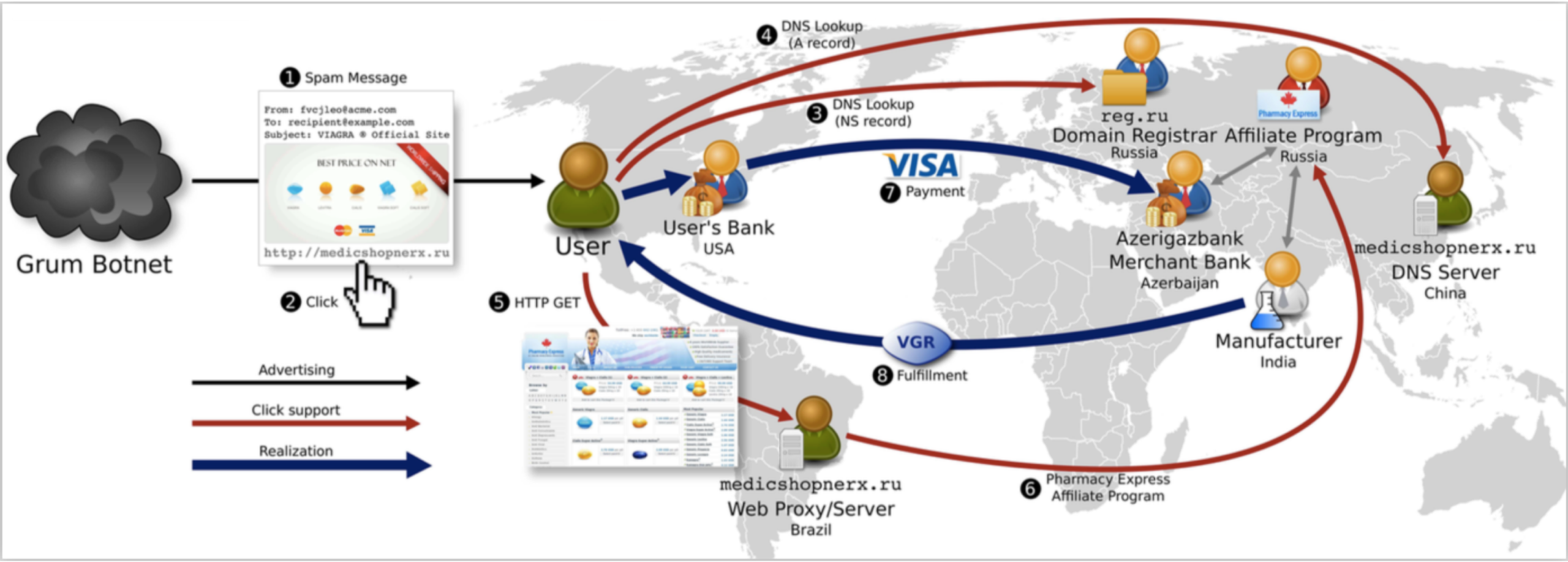
- Infection prevention
- Infection detection
- C&C take-down
- Undermine the economics
  - Banking take-down



Studying grey/black market products

- Active measurement studies to:
  - Understand (probably illicit) services on web
  - Find ways to defuse underground markets
- Previous studies looked at botnets themselves and victims
- Let’s look at the “backend”

Example spam-advertised goods backend



From Levchenko et al., “Click Trajectories: End-to-End Analysis of the Spam Value Chain”, IEEE Symposium on Security and Privacy, 2011

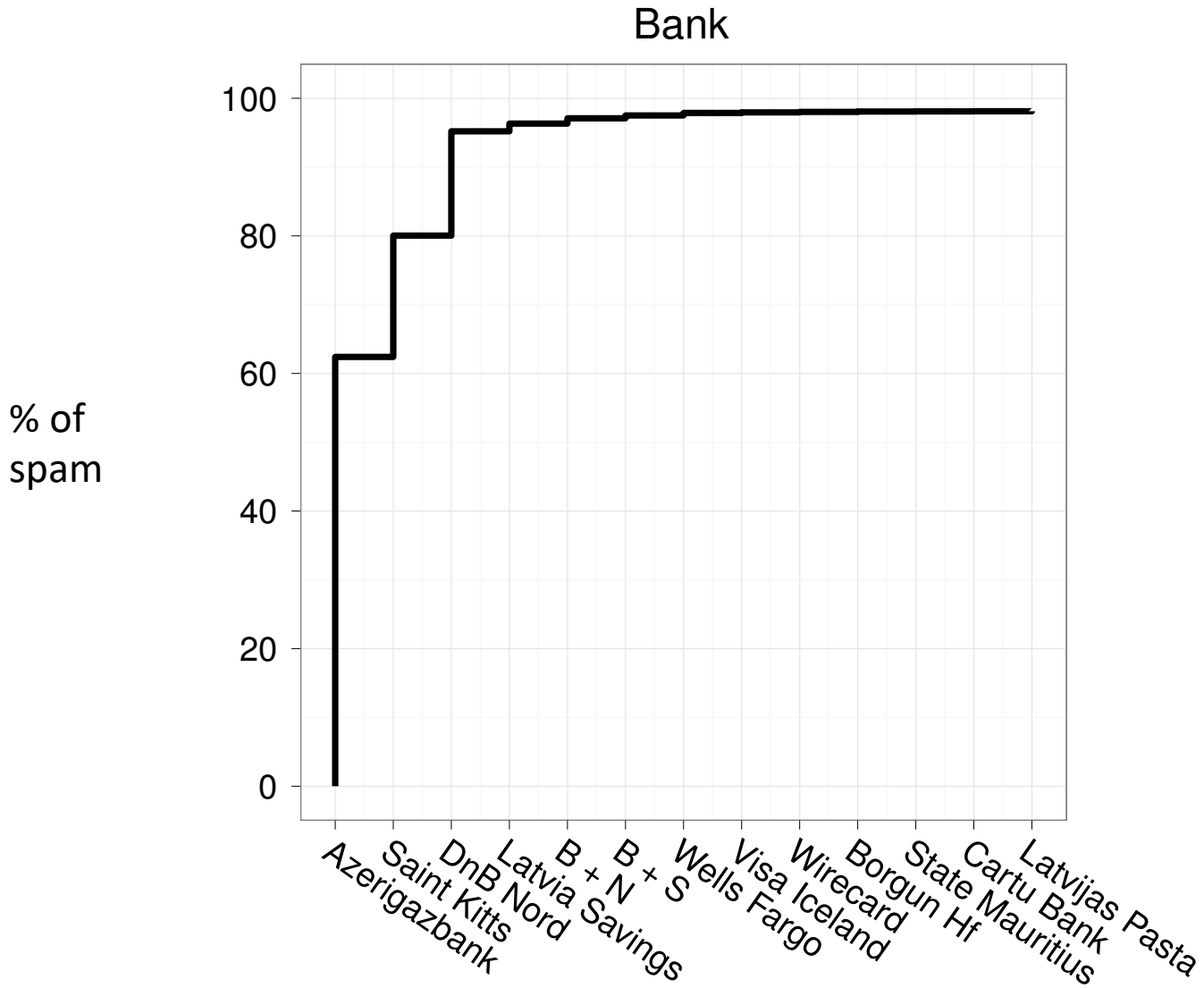
- 120 items purchased
- 76 authorized
- 56 settled
- 49 products delivered

- 2 sent after mailbox lease ended
- 2 no follow-up email
- 2 resent after mailbox lease ended
- 1 promised refund (never obtained)

Supplier	*Item*	*Origin*	*Affiliate Programs*
Aracoma Drug	Orange bottle of tablets (pharma)	WV, USA	ClFr
Combitic Global Caplet Pvt. Ltd.	Blister-packed tablets (pharma)	Delhi, India	GlvMd
M.K. Choudhary	Blister-packed tablets (pharma)	Thane, India	OLPh
PPW	Blister-packed tablets (pharma)	Chennai, India	PhEx, Stmul, Trust, ClFr
K. Sekar	Blister-packed tablets (pharma)	Villupuram, India	WldPh
Rhine Inc.	Blister-packed tablets (pharma)	Thane, India	RxPrm, DrgRev
Supreme Suppliers	Blister-packed tablets (pharma)	Mumbai, India	Eva
Chen Hua	Small white plastic bottles (herbal)	Jiangmen, China	Stud
Etech Media Ltd	Novelty-sized supplement (herbal)	Christchurch, NZ	Staln
Herbal Health Fulfillment Warehouse	White plastic bottle (herbal)	MA, USA	Eva
MK Sales	White plastic bottle (herbal)	WA, USA	GlvMd
Riverton, Utah shipper	White plastic bottle (herbal)	UT, USA	DrMax, Grow
Guo Zhonglei	Foam-wrapped replica watch	Baoding, China	Dstn, UltRp

Table VI: List of product suppliers and associated affiliate programs and/or store brands.

Levchenko et al., Click Trajectories: An End-to-End Analysis of the Spam Value Chain, 2011



Levchenko et al., Click Trajectories: An End-to-End Analysis of the Spam Value Chain, 2011

Targeting merchant accounts at banks

- [McCoy et al., Priceless: The Role of Payments in Abuse-advertised Goods, 2012]
- Made purchases to pharma and software OEM programs, while also working with brandholders to make complaints to Visa/MC

> Wrote one eloquent affiliate in March of this year, "Right now most affiliate eprograms have a mass of declines, cancels and pendings, and it doesn't depend much on the program IMHO, there is a general sad picture, f!$#@ing Visa is burning us with napalm."

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, September 10, 2019

281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes

74 Alleged Fraudsters Arrested in the United States

https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds

How to prevent fraudulent actions?

- **Content analysis**
  - Spam filters
- **Identify bad accounts**
  - Correlate bad actions with accounts, try to detect bots
  - Sock-puppet accounts (many controlled by one person)
- **Identify bad devices**
  - Device cookies to correlate different account accesses
  - IP blacklists, ISP blacklists
- **Target fraud-support infrastructure**
  - Botnet takedowns, bank accounts, civil/criminal legal actions

E-crime is a complex ecosystem

- Lots of moving parts
- Economics important
  - Fascinating measurement studies
- Technical mechanisms often don't measure up
- "In Planning Digital Defenses, the Biggest Obstacle Is Human Ingenuity" -Stefan Savage
  - http://www.nytimes.com/2011/12/06/science/stefan-savage-girding-for-digital-threats-we-havent-imagined-yet.html?_r=1&ref=science

Botnet measurement methods

Technique	Description	Pros	Cons
Monitor endpoint	monitor traffic of a bot	simple, generally applicable	limited view, encryption
Internet telescopes	monitor random-scan infection attempts	botnet-wide view	limited applicability
Monitor IRC	record IRC C&C traffic	simple, botnet-wide view	only IRC botnets
DNS redirect	hijack C&C via DNS	measure infection size	limited applicability
Sybil monitoring	monitor numerous bots	simple, passive	resource-intensive, limited view, structured P2P
Botnet crawling	crawl botnet overlay	enumerate large portion of botnet	detectable
DNS cache probing	probe DNS caches for botnet C&C	simple, passive	loose lower-bound
DNSBL counter-intelligence	sniff DNSBL traffic, heuristically identify bots	passive	limited applicability
Flow analysis	detect botnets via flow-based anomaly detection	wide-scale, handles encryption	tailored to IRC botnets

Size estimates from literature as of 2008

Study	Method(s) used	C&C's observed	Largest botnet size infection	Largest botnet size effective	Total # of infected hosts
[13]	IRC monitoring	∼100	226,585	–	–
[8]	IRC monitoring	∼180	∼50,000	–	∼300,000
[22]	DNS cache probing	65	–	–	85,000
	IRC monitoring	>100	>15,000	∼3,000	–
[23]	DNS cache probing	100	–	–	88,000
	IRC monitoring	472	∼100,000	>10,000	426,279
[5]	DNS redirection	∼50	>350,000	–	–
[15]	flow analysis	∼376	–	–	∼6,000,000
[7]	botnet crawling	1	∼160,000	∼44,000	–

Figure 2: Size estimates from the literature. All sizes are the maximum ones given in the appropriate study and the final column represents the total number of infected hosts over all botnets encountered.

Overnet DHT

DHT stands for Distributed Hash Table

Peer-to-peer protocol for storing and retrieving data

Storm uses DHT to store IP addresses of proxies

Proxies maintain contact withBot C&C servers

Publicly addressable bots advertise as able to C&C proxy

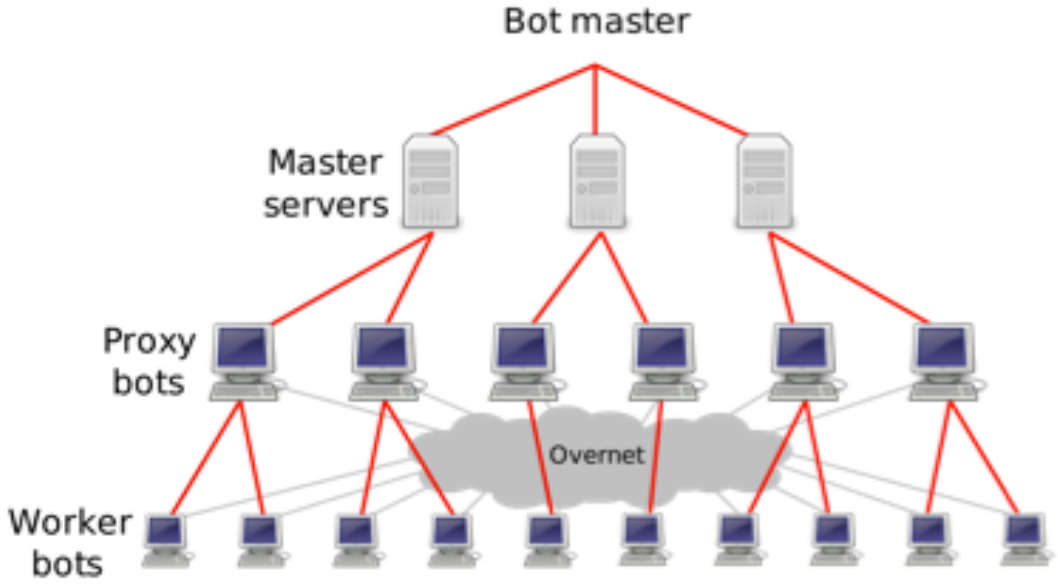


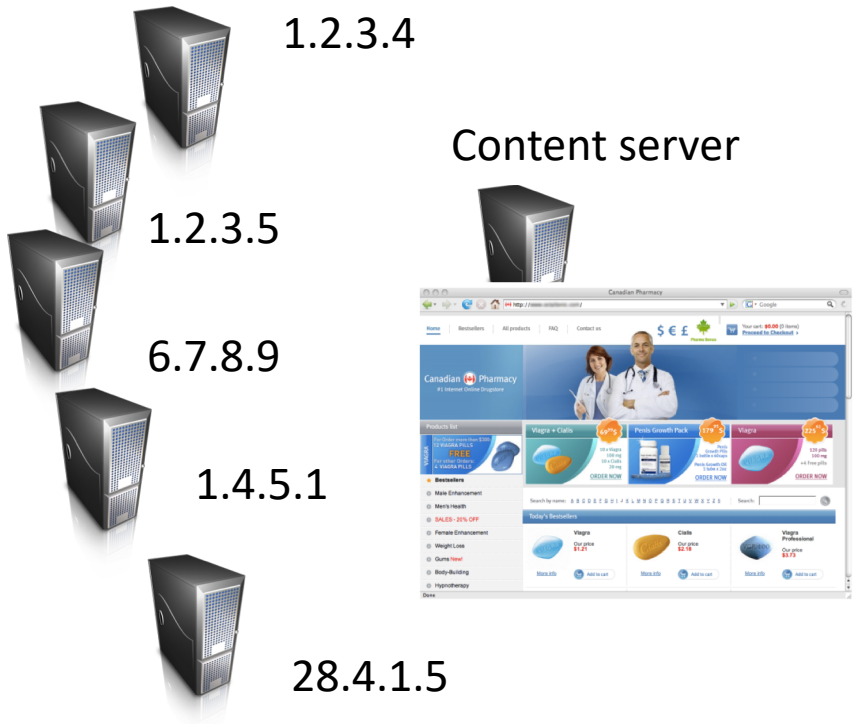
Figure 1: The Storm botnet hierarchy.

Fast-flux DNS

Spam campaign that directs users to ***pharmashop.com***

Single flux:

- Change A (address) record for ***pharmashop.com*** quickly to point to different compromised systems
- Short TTL (e.g., 5 minutes)

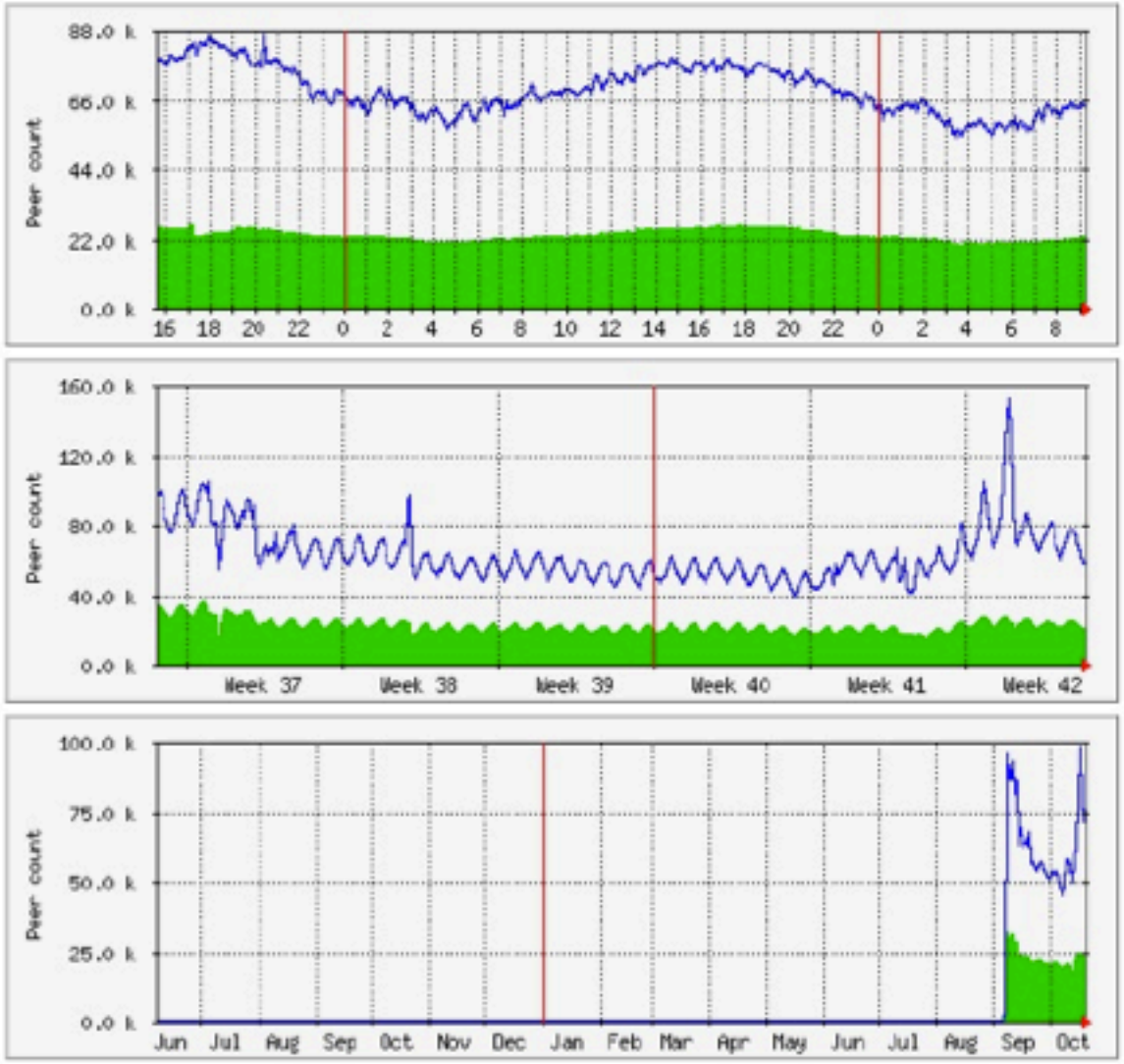


Double flux:

- Change NS (nameserver) record for ***pharmashop.com*** to point to different compromised systems

Similar to round-robin DNS as used by major websites

Size of Storm botnet



The blue peers count is all peers being probed at a time. This includes live, active, dead, and unknown states. The peers line is not the size of the network. The active line is much closer to the instantaneous size of the network.

It can be seen in the month and year chart that Microsoft made a measurable dent in the network with the MRT Storm (Nuwar) release.

```
;; ANSWER SECTION:
images.pcworld.com.                    900     IN    CNAME   images.pcworld.com.edgesuite.net.
images.pcworld.com.edgesuite.net.    21600     IN    CNAME   a1694.g.akamai.net.
a1694.g.akamai.net.                     20     IN    A       212.201.100.135
a1694.g.akamai.net.                     20     IN    A       212.201.100.141
```

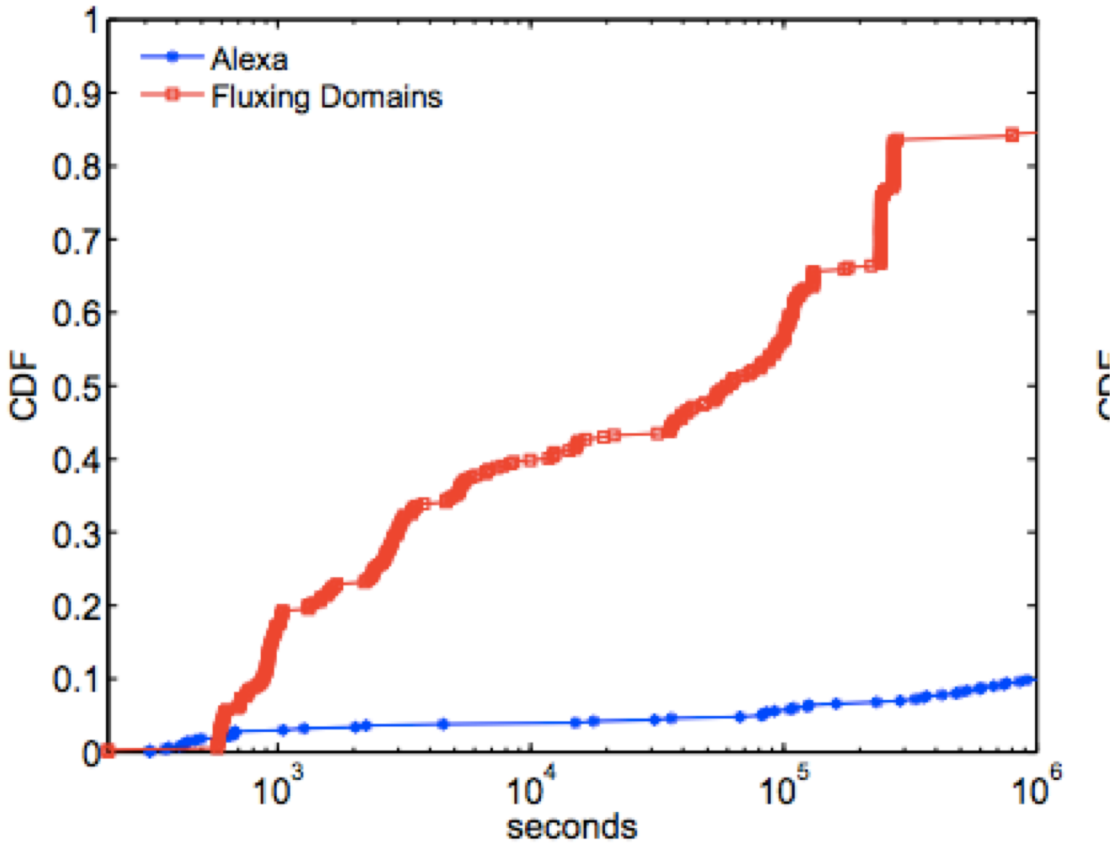
```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       69.183.26.53
thearmynext.info.       600     IN      A       76.205.234.131
thearmynext.info.       600     IN      A       85.177.96.105
thearmynext.info.       600     IN      A       217.129.178.138
thearmynext.info.       600     IN      A       24.98.252.230
```

```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       213.47.148.82
thearmynext.info.       600     IN      A       213.91.251.16
thearmynext.info.       600     IN      A       69.183.207.99
thearmynext.info.       600     IN      A       91.148.168.92
thearmynext.info.       600     IN      A       195.38.60.79
```

Holz et al. 2008
http://pi1.informatik.uni-mannheim.de/filepool/publications/fast-flux-ndss08.pdf

Studying fast-flux

CDF of average time between DNS A record address changes



(a) A records

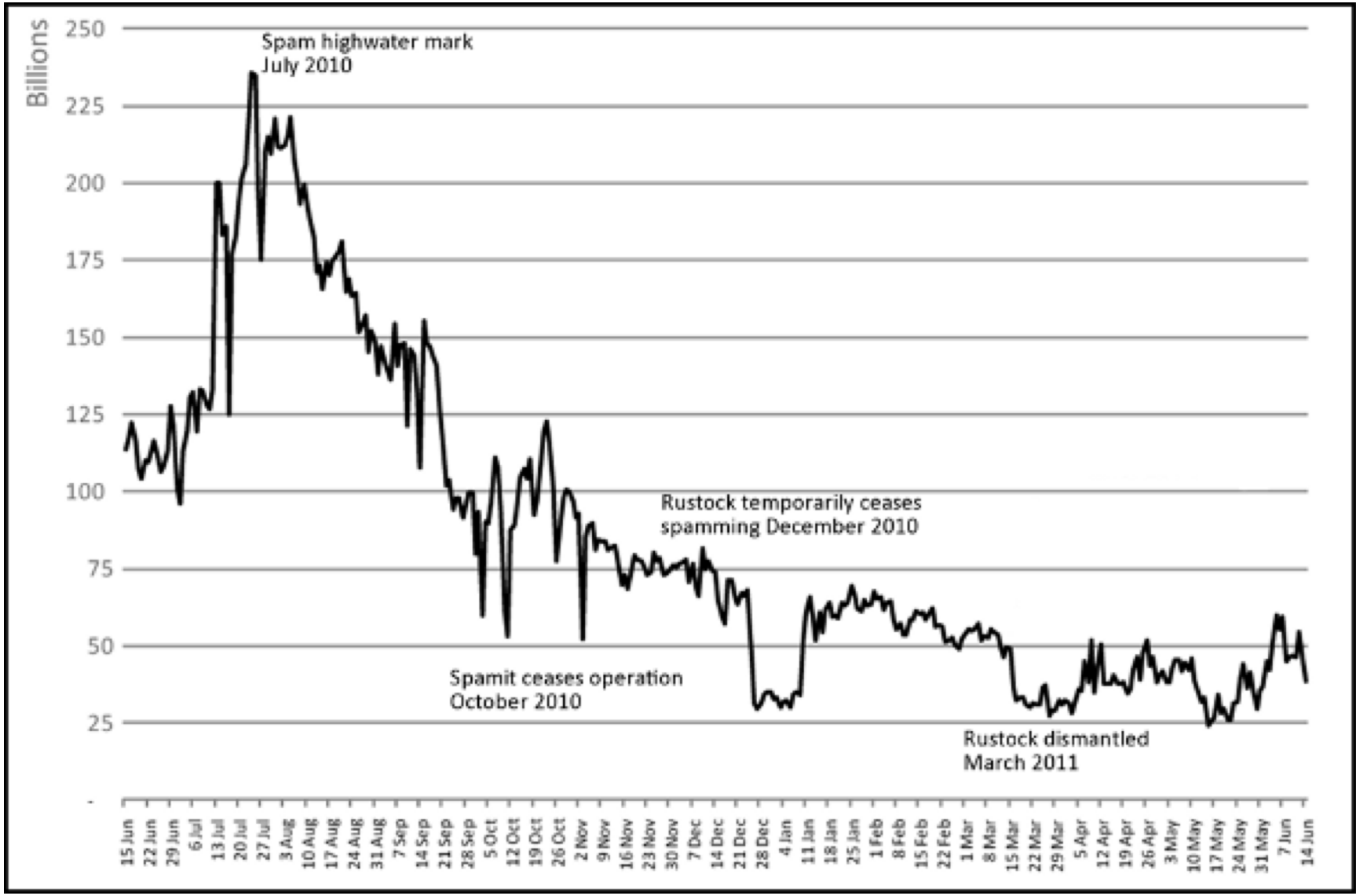
Konte et al. 2008
http://www.cc.gatech.edu/~feamster/papers/fastflux-tr08.pdf

Studying fast-flux

Table 1: Change Rate of Monitored FF Domains

type	Minutes/IP	IP/Day	A-TTL	NS-TTL
average	73.55	55.90	1832.84	37348.75
max	634.50	261.54	21598.03	65535.00
min	5.51	2.27	0	0

Xu et al. 2013
https://media.blackhat.com/us-13/US-13-Xu-New-Trends-in-FastFlux-Networks-WP.pdf



http://www.symantec.com/connect/blogs/why-my-email-went

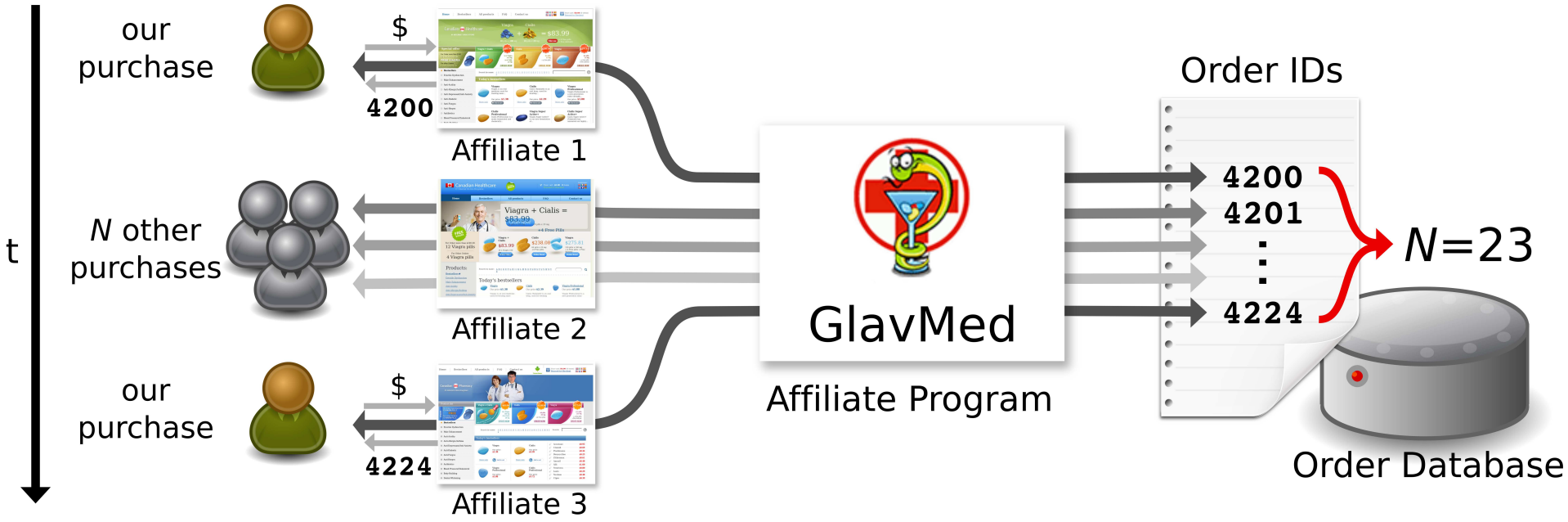
Spam-advertised products

- Pharmaceuticals
- Software
- Watches
- etc.

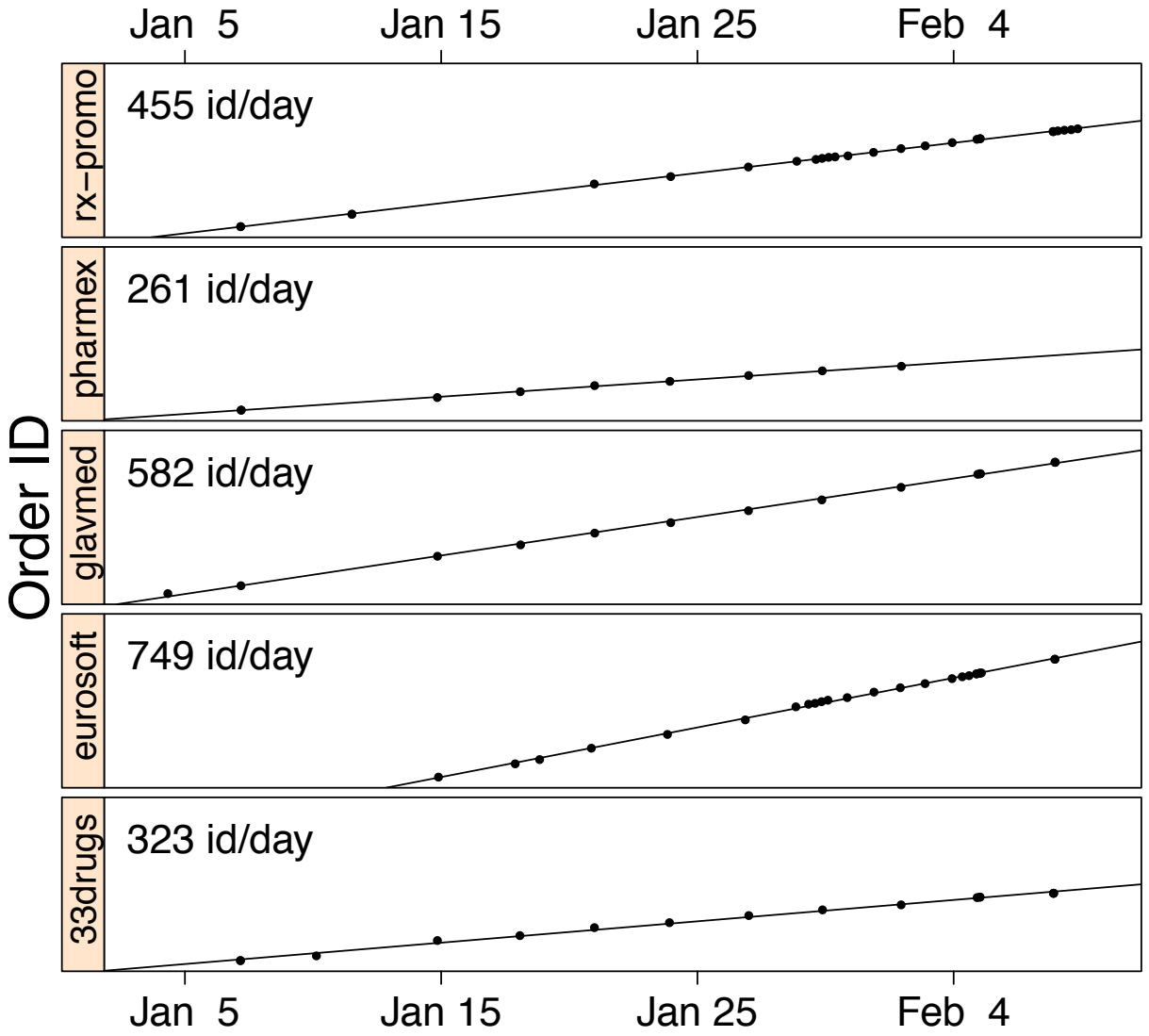
http://www.rioricopharmacy.com/

- What is order volume?
- What kinds of things are being purchased?
- What are weak links for disruption?

Measurement apparatus #1

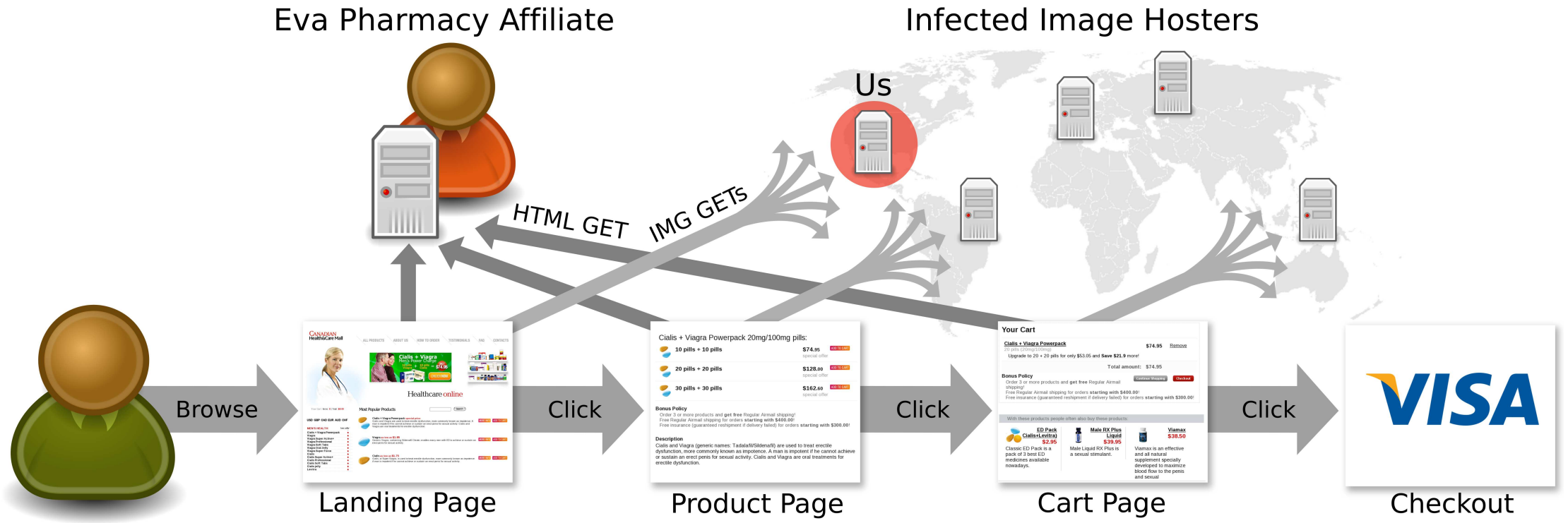


Kanich et al., Show Me the Money: Characterizing Spam-advertised Revenue, 2011



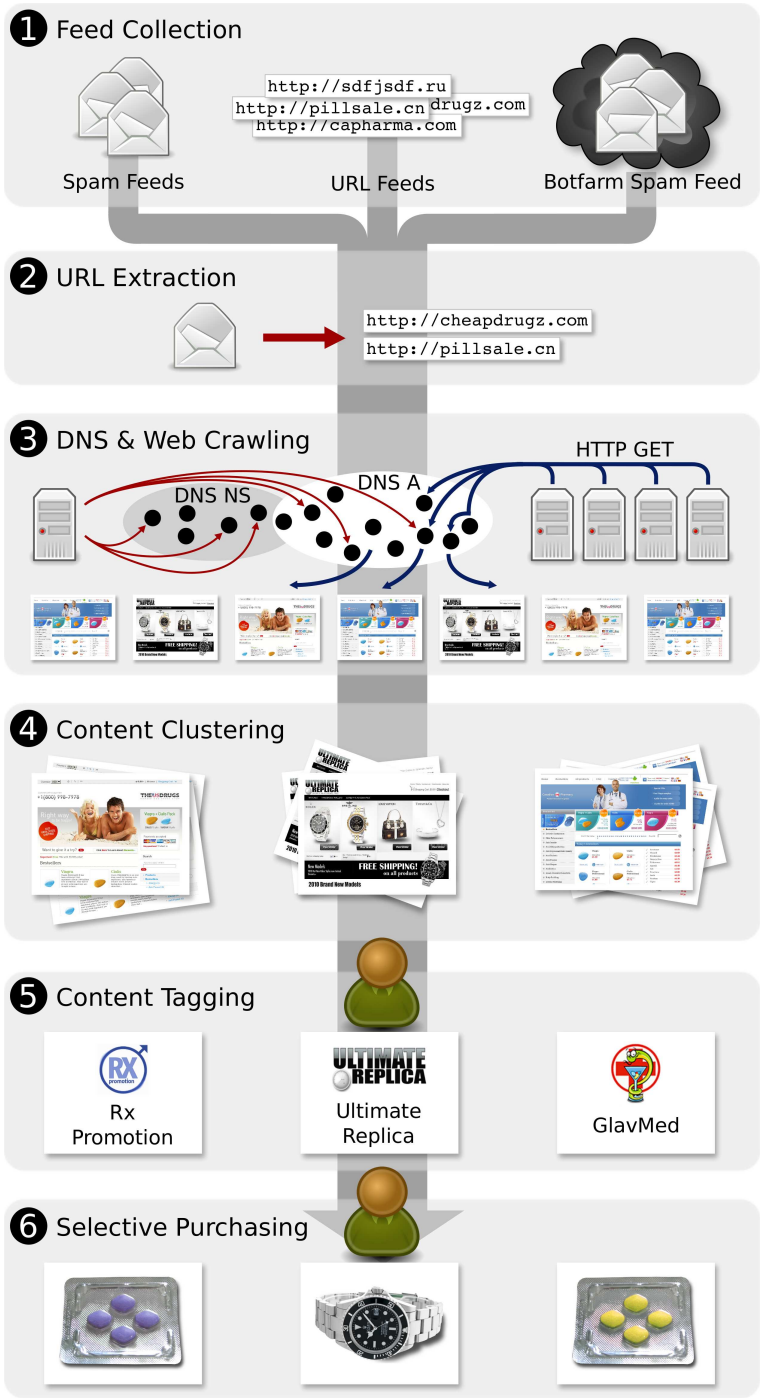
Kanich et al., Show Me the Money: Characterizing Spam-advertised Revenue, 2011

Measurement Apparatus #2



Product	Quantity	Min order
Generic Viagra	568	$78.80
Cialis	286	$78.00
Cialis/Viagra Combo Pack	172	$74.95
Viagra Super Active+	121	$134.80
Female (pink) Viagra	119	$44.00
Human Growth Hormone	104	$83.95
Soma (Carisoprodol)	99	$94.80
Viagra Professional	87	$139.80
Levitra	83	$100.80
Viagra Super Force	81	$88.80
Cialis Super Active+	72	$172.80
Amoxicillin	47	$35.40
Lipitor	38	$14.40
Ultram	38	$45.60
Tramadol	36	$82.80
Prozac	35	$19.50
Cialis Professional	33	$176.00
Retin A	31	$47.85

Kanich et al., Show Me the Money: Characterizing Spam-advertised Revenue, 2011



Levchenko et al., Click Trajectories: An End-to-End Analysis of the Spam Value Chain, 2011