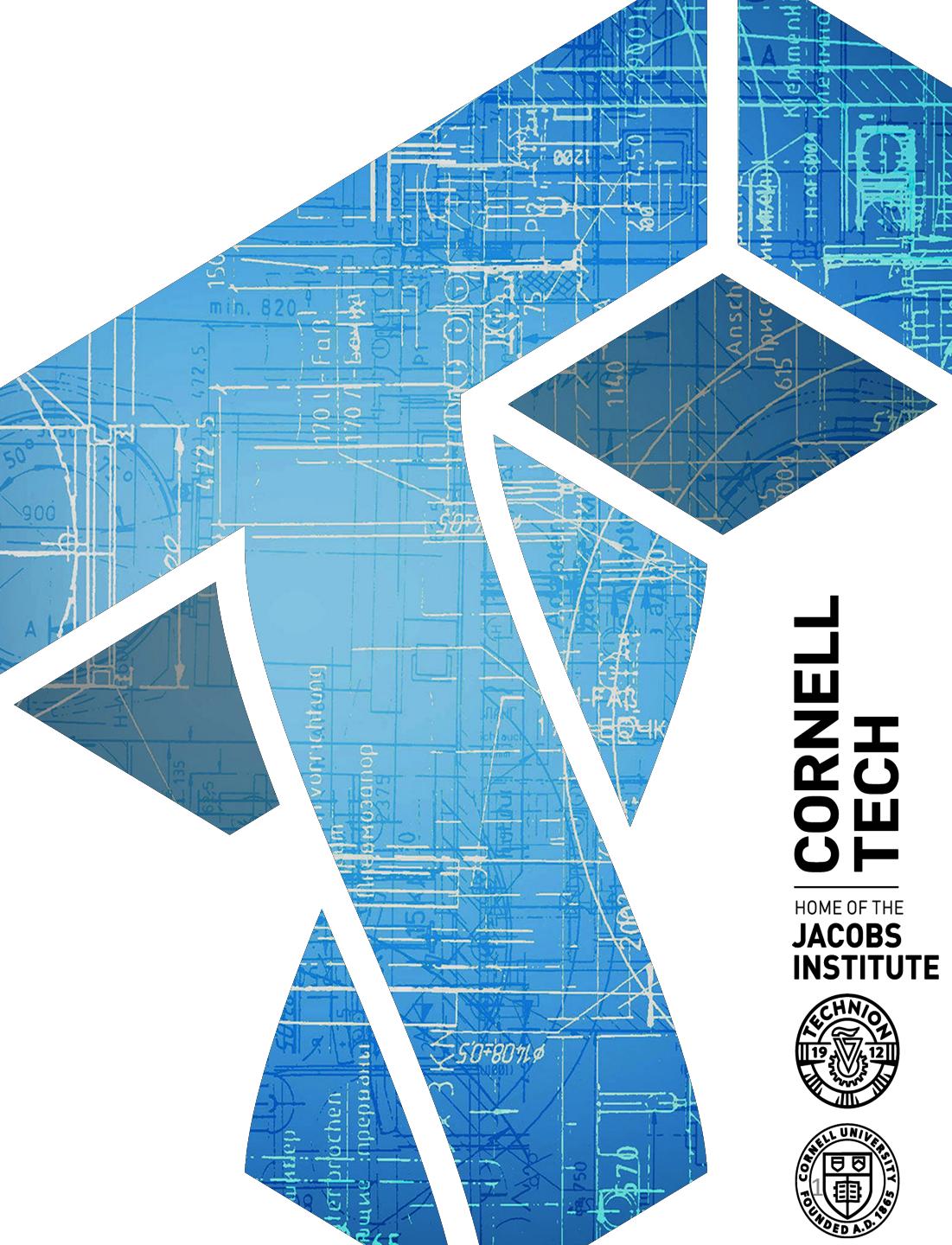


CS 5435: Commercially- motivated abuse

Instructor: Tom Ristenpart

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



Airbnb as an example service



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

Official request

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

J

Reply-To: jocun01250@mail2banker.com

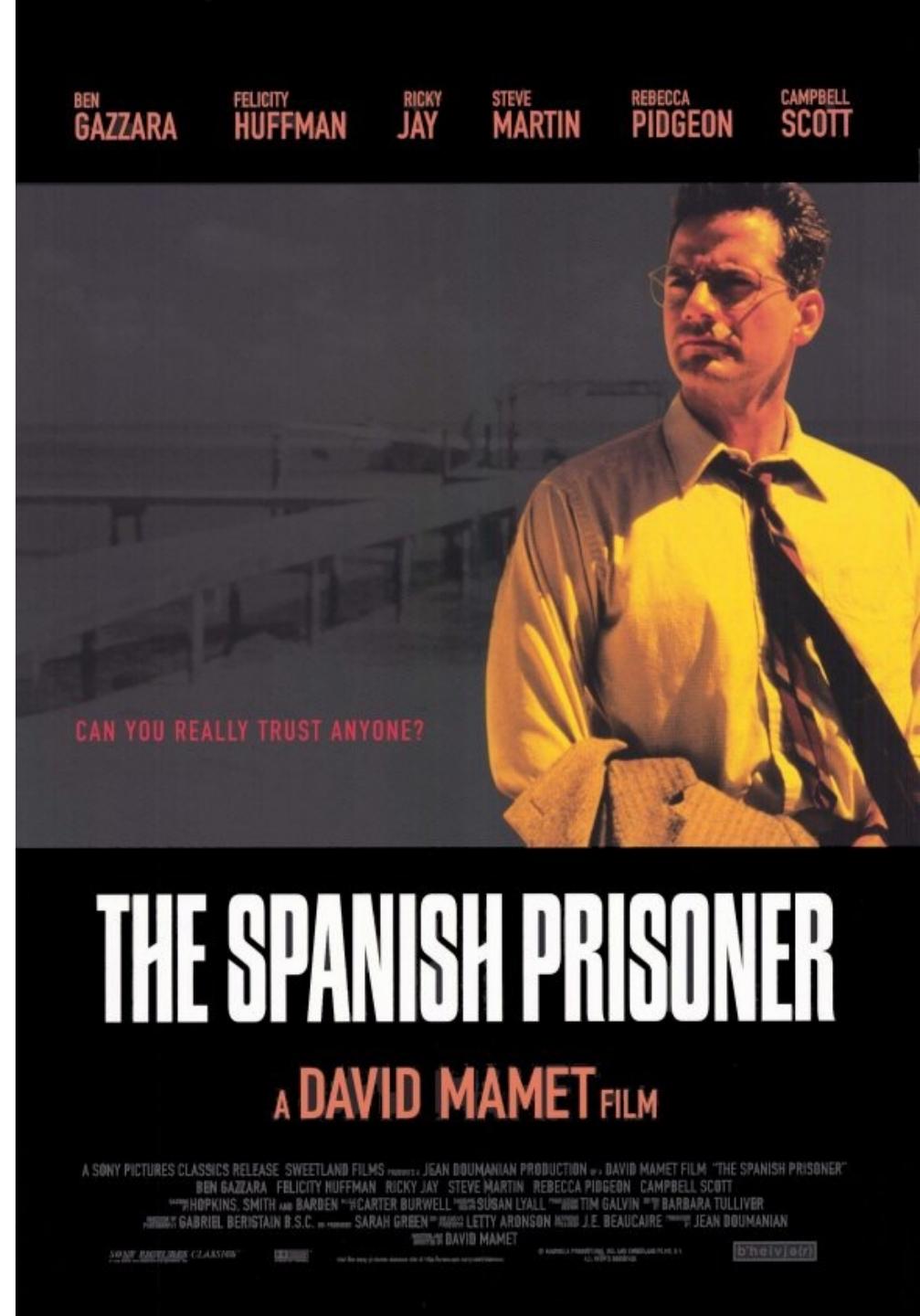
Hello,

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*



By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Descriptors*

Cryptocurrency	31,310	Cryptocurrency Wallet	20,781
----------------	--------	-----------------------	--------

By Victim Loss

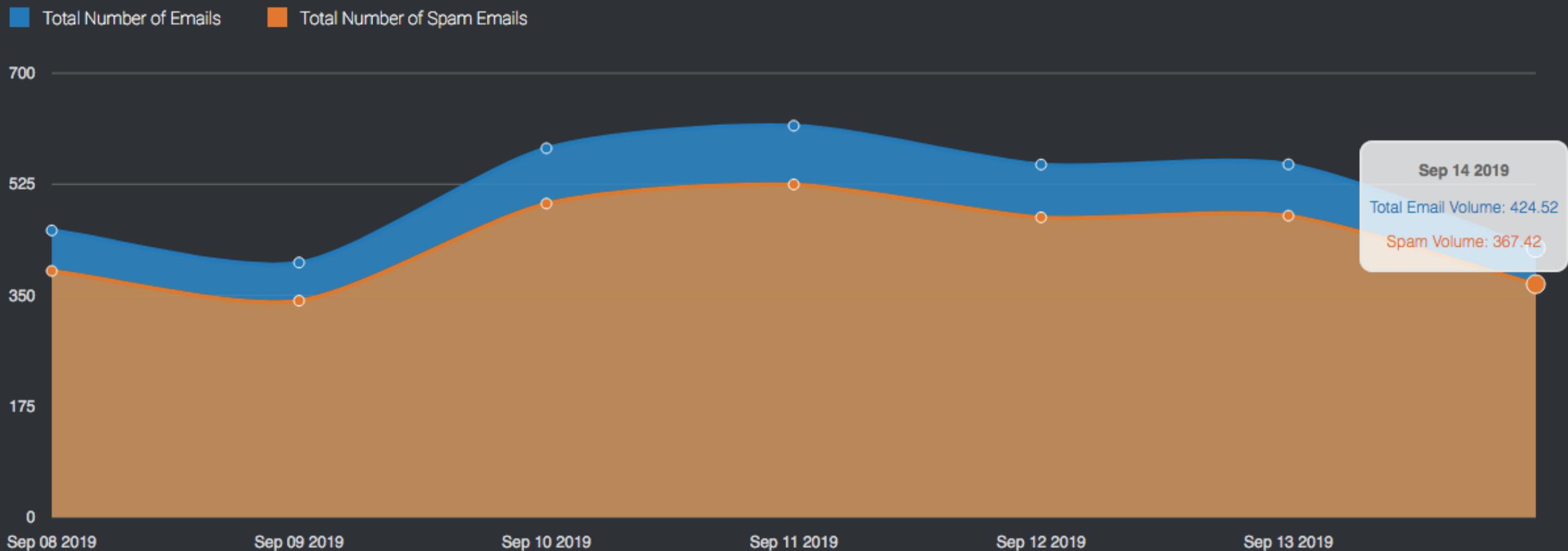
Crime Type	Loss	Crime Type	Loss
Investment	\$3,311,742,206	Lottery/Sweepstakes/Inheritance	\$83,602,376
BEC	\$2,742,354,049	SIM Swap	\$72,652,571
Tech Support	\$806,551,993	Extortion	\$54,335,128
Personal Data Breach	\$742,438,136	Employment	\$52,204,269
Confidence/Romance	\$735,882,192	Phishing	\$52,089,159
Data Breach	\$459,321,859	Overpayment	\$38,335,772
Real Estate	\$396,932,821	Ransomware	*\$34,353,237
Non-Payment/Non-Delivery	\$281,770,073	Botnet	\$17,099,378
Credit Card/Check Fraud	\$264,148,905	Malware	\$9,326,482
Government Impersonation	\$240,553,091	Harassment/Stalking	\$5,621,402
Identity Theft	\$189,205,793	Threats of Violence	\$4,972,099
Other	\$117,686,789	IPR/Copyright/Counterfeit	\$4,591,177
Spoofing	\$107,926,252	Crimes Against Children	\$577,464
Advanced Fee	\$104,325,444		

Descriptors**

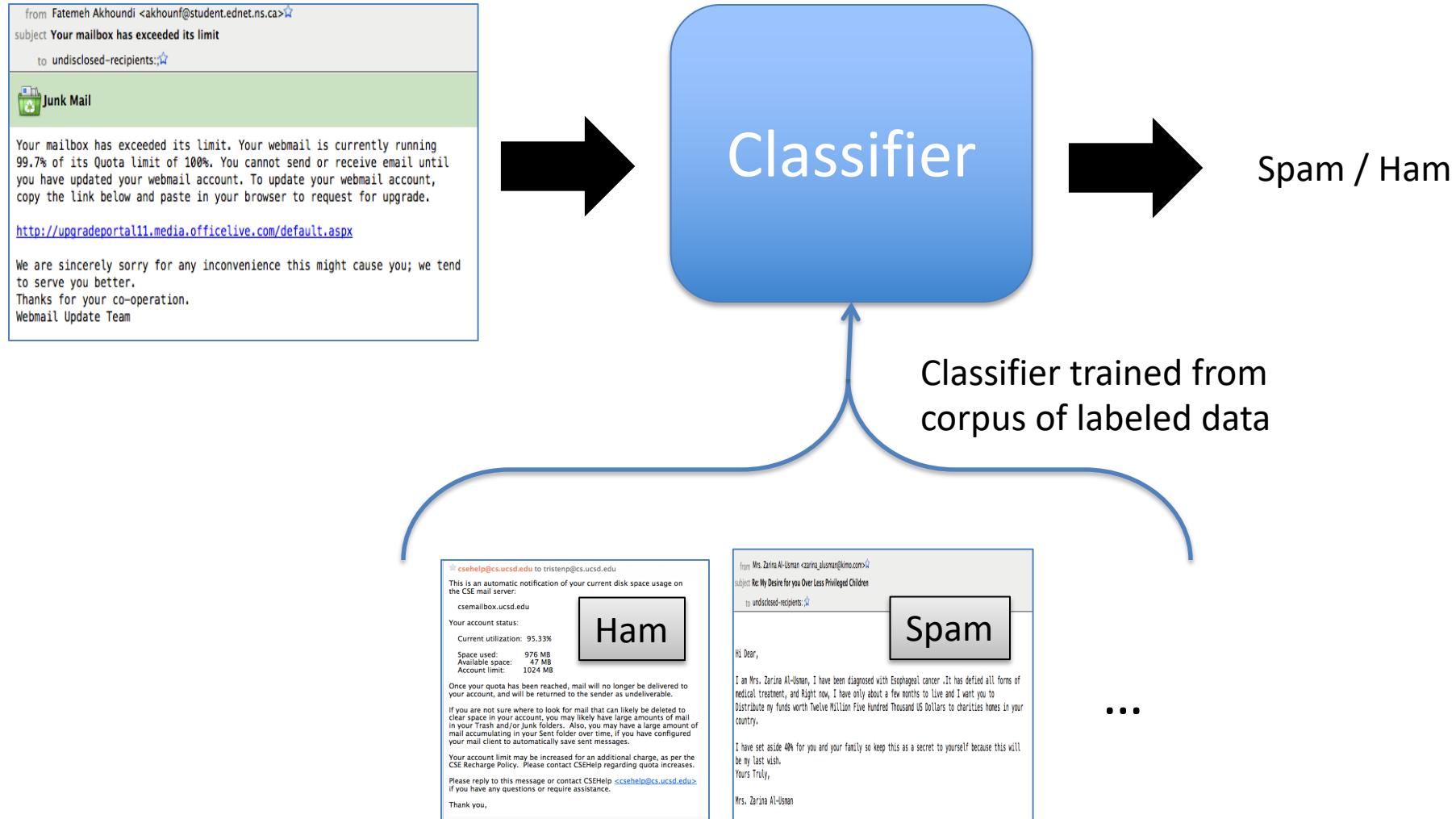
Cryptocurrency	\$2,496,196,530	Cryptocurrency Wallet	\$1,349,090,883
----------------	-----------------	-----------------------	-----------------

GLOBAL EMAIL VOLUME IN BILLIONS

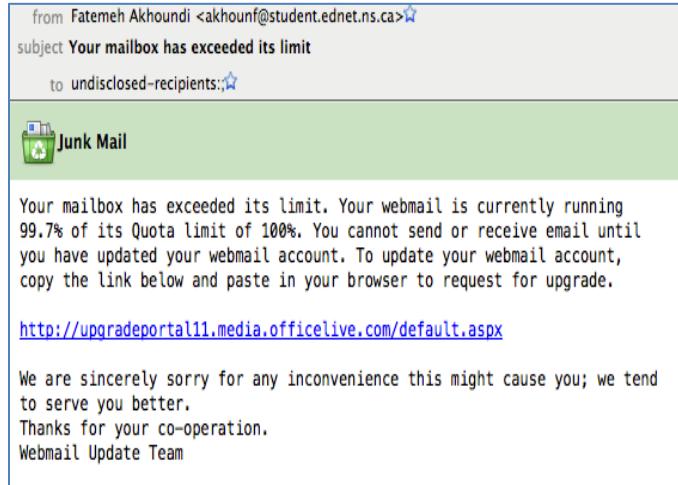
LAST WEEK ▾



Spam Classifiers



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
:	:	

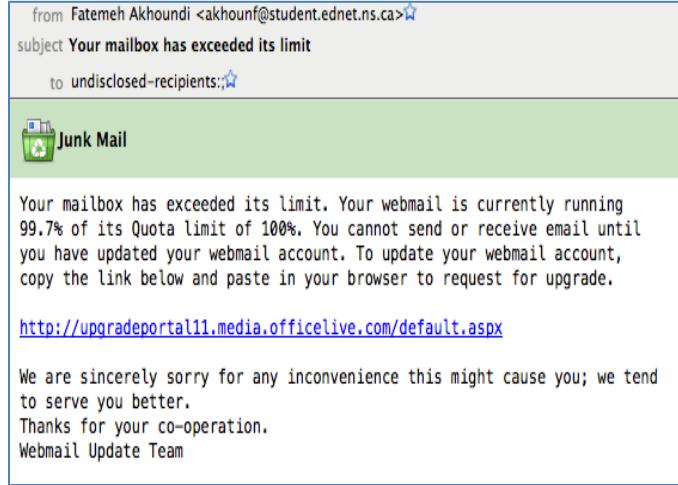
Intuition: spam and ham have different distribution of keywords

$$\Pr[\text{spam} \mid x_1, x_2, \dots, x_n] = \frac{\Pr[x_1, x_2, \dots, x_n \mid \text{spam}] \Pr[\text{spam}]}{\Pr[x_1, x_2, \dots, x_n]} \quad \text{Bayes' theorem}$$

$$= \frac{\Pr[\text{spam}] \prod \Pr[x_i \mid \text{spam}]}{\Pr[x_1, x_2, \dots, x_n]} \quad \text{"Naïve": assume words independent}$$

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

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
:	:	

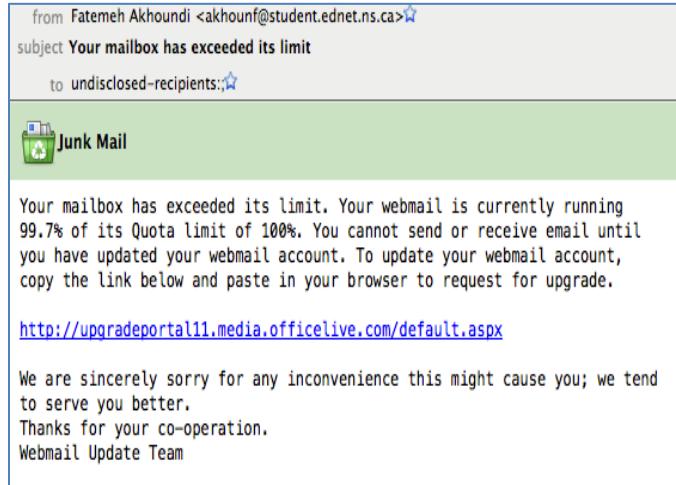
Intuition: spam and ham have different distribution of keywords

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

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

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

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

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

Estimate these from labeled training data

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

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)

Phishing and spearphishing

- Sending emails / SMS / chats to get target to reveal personal information
- Spearphishing: tailored phishing attack against target
- Phishing often bypasses filtering mechanisms

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183

Phishing and spearphishing

- Sending emails / SMS / chats to get target to reveal personal information
- Spearphishing: tailored phishing attack against target
- Phishing often bypasses filtering mechanisms

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183



+27 67 268 5729



Apr 11, 2023

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. [Click to learn more.](#)



Hi.
2:39 PM

Wed, Nov 15

You blocked this contact. Click to unblock.

What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One.

<https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one>

Thousands have lost huge sums after being lured into fraudulent online investment schemes by seemingly attractive strangers who strike up online conversations with them. Here's a guide to spotting the telltale signs.

1. Create fake identity
2. Make contact
3. Win trust
4. Sign target up for investment
5. Real money into fake account
6. “Prove” investment working
7. Manipulate to invest more
8. Cut them off
9. Exploit desperation
10. Taunt and depart

Web services in-class exercise



Google



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

"30 days unlimited traffic"

Stop getting scammed from traffic sellers!
This is real quality traffic that
We use for own sites.



INCREASE WEB TRAFFIC
GUARANTEED!

REVISITORS.com

Targeted Traffic Since 2005



TOLL FREE:

877.389.3330

101 California St - San Francisco, CA

How it Works Order

Testimonials

Affiliates

Blog

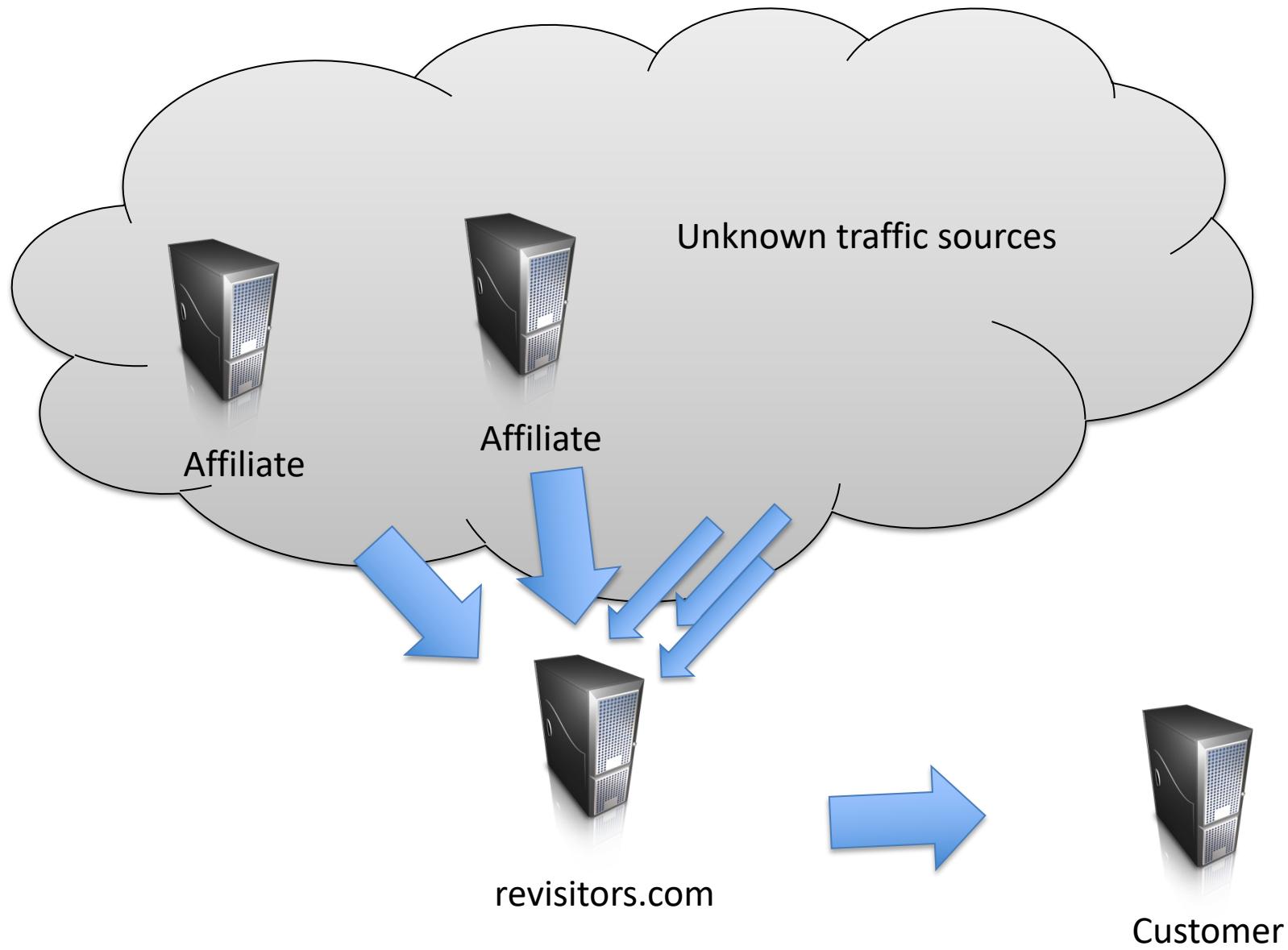
FAQ

Support

Members



You can't make **Sales** if don't have **VISIToRS**



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

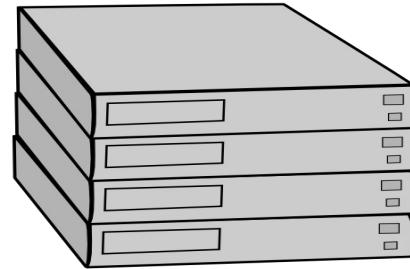
Traffic resellers: resell purchased traffic

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 =====

qu

Hello Tom,

A staff member has replied to your question:

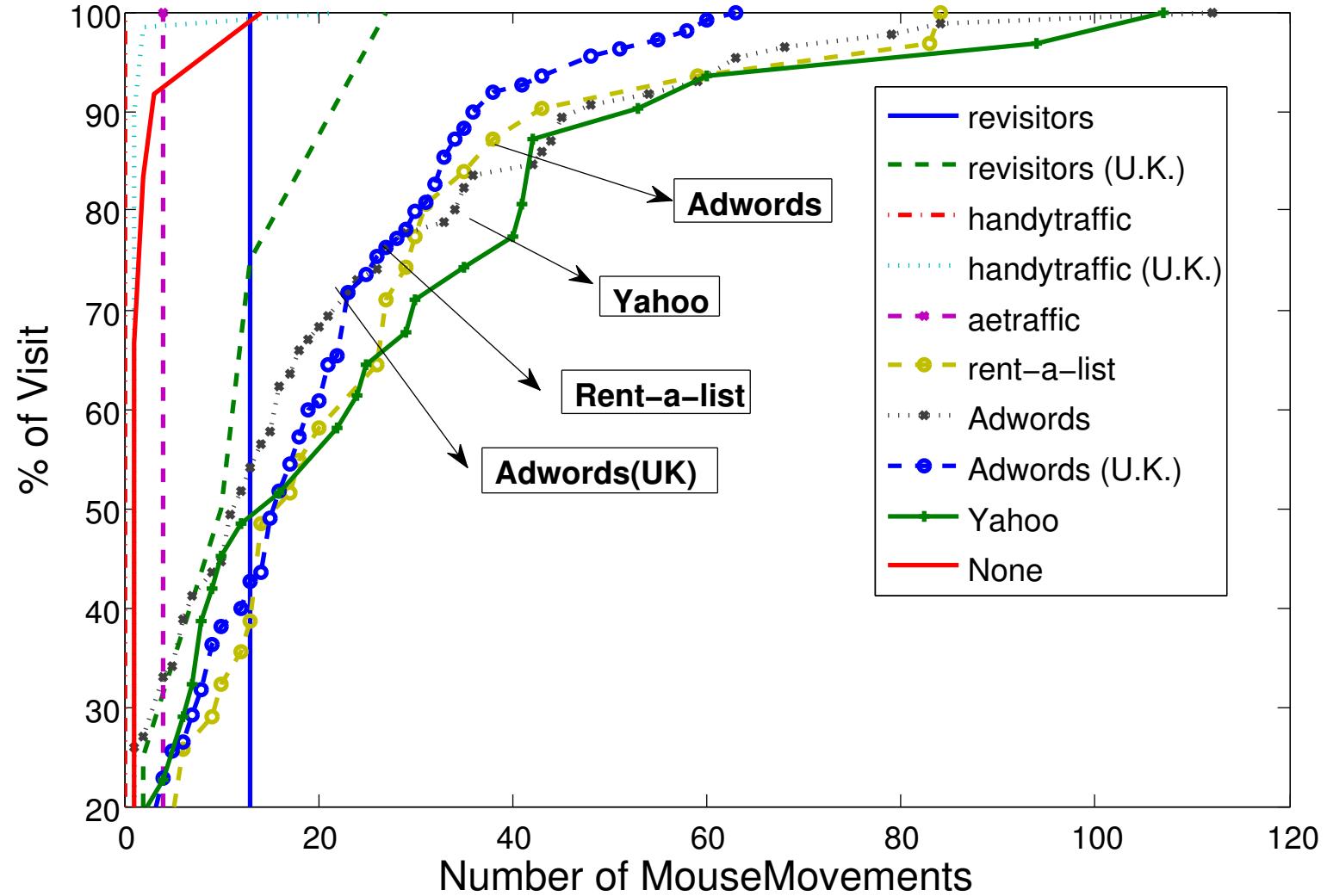
Dear Tom,

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>

W



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

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, ...

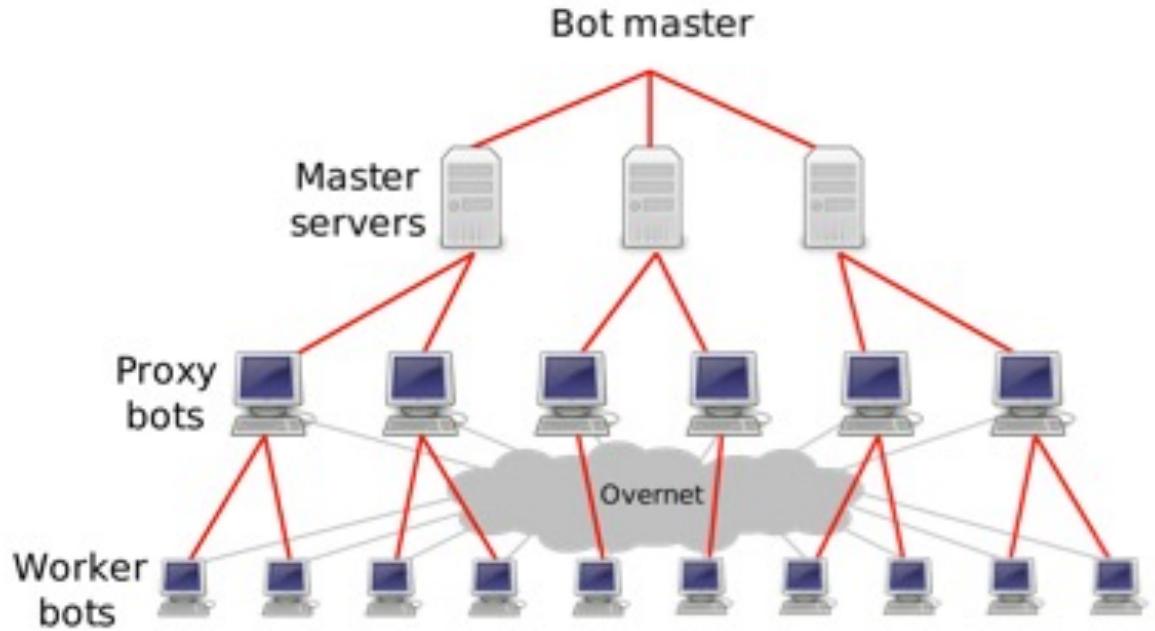


Figure 1: The Storm botnet hierarchy.

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

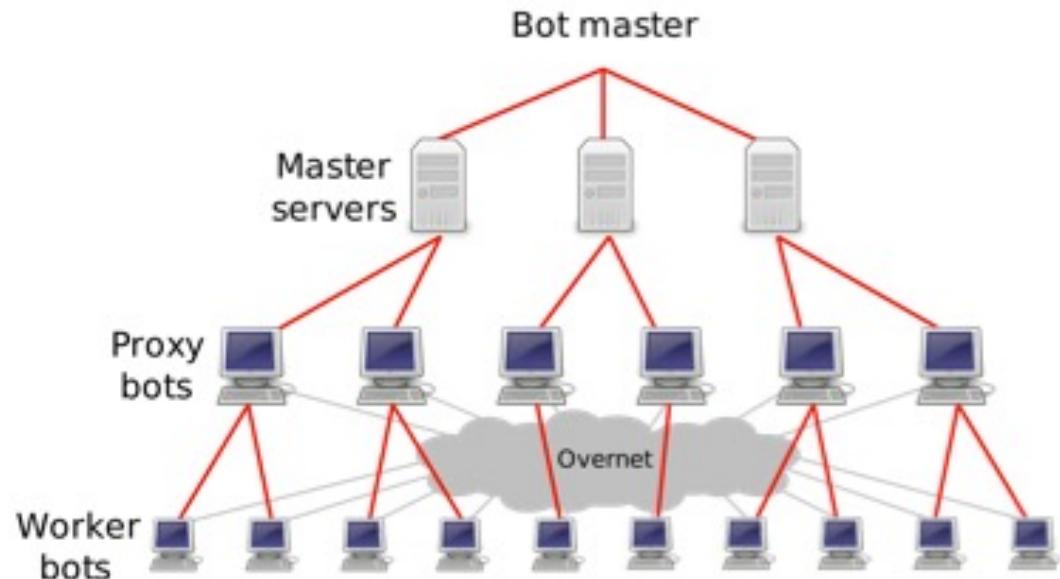


Figure 1: The Storm botnet hierarchy.

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]

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		Users		Top Subcategory
	B	S	B	S	
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 svrs	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 <chill@hetajobs.com>★

 reply

subject Cool Student Job

to pubs@cs.wisc.edu★

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

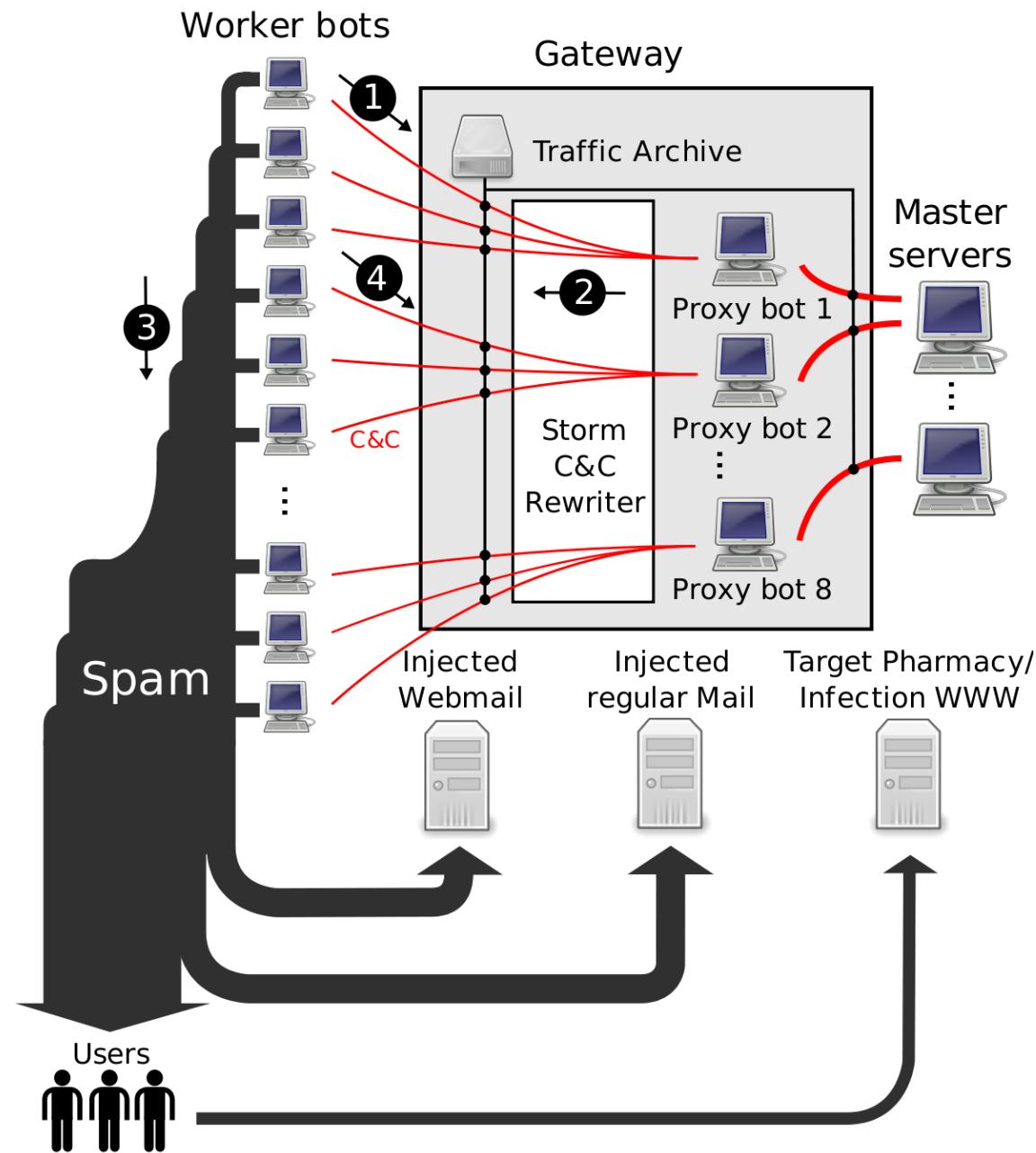


Organized cyber criminals stole almost \$11 million in two highly coordinated ATM heists in the final days of 2012, KrebsOnSecurity has learned. The events prompted **Visa** to warn U.S. payment card issuers to be on high-alert for additional ATM cash-out fraud schemes in the New Year.

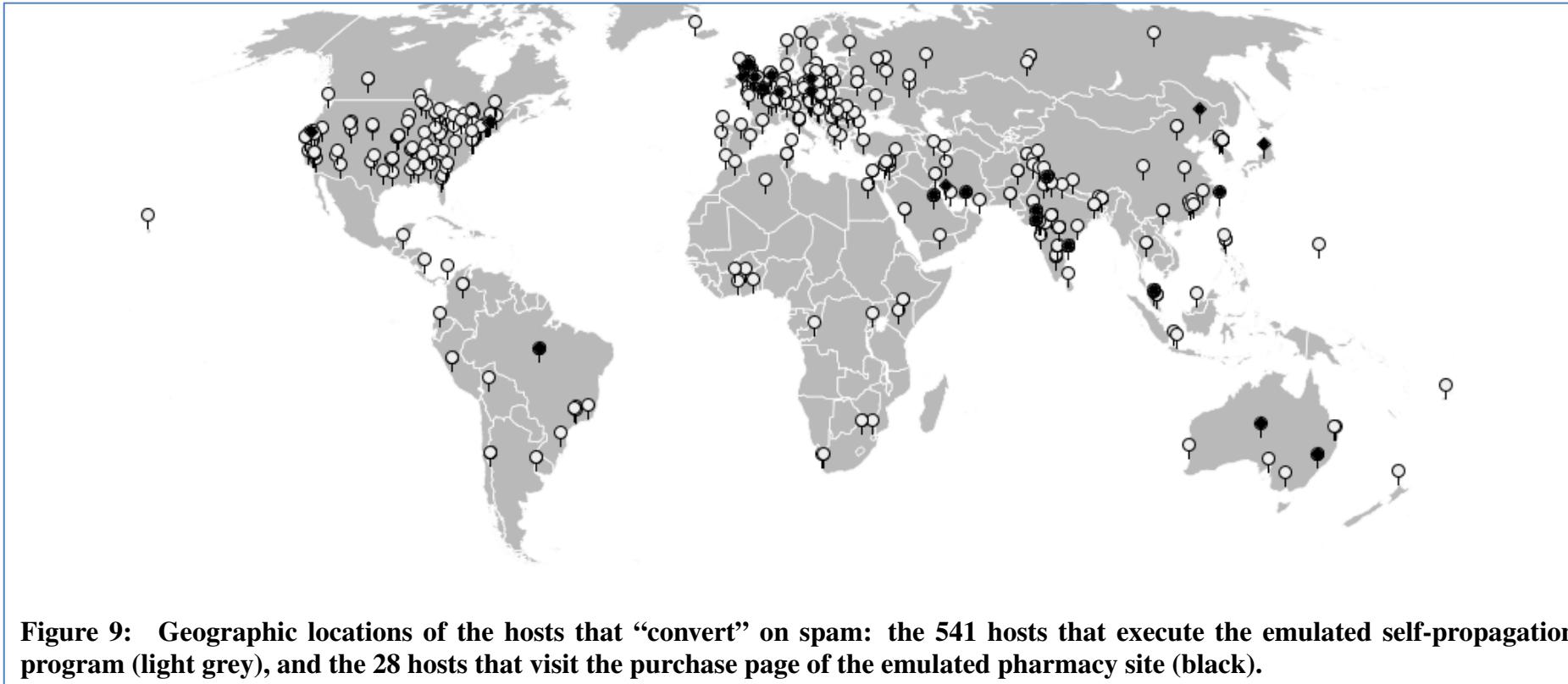


Botnet takeover studies

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



The victims



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

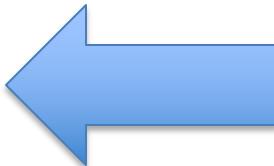
BY KIM ZETTER 03.26.12 2:45 PM

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?

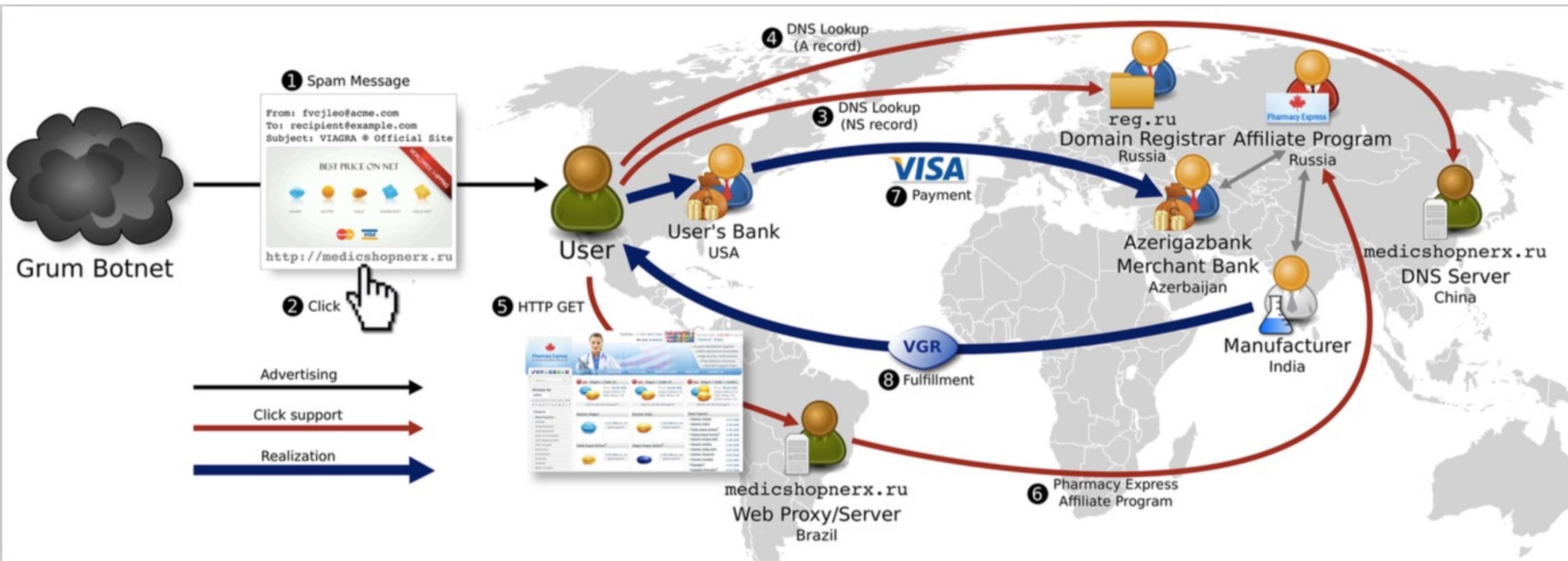
- Infection prevention
- Infection detection
- C&C take-down
- Undermine the economics
 - Banking take-down



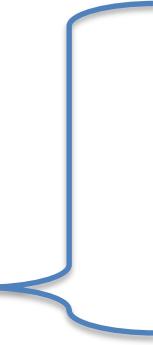
Studying grey/black market products

- 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

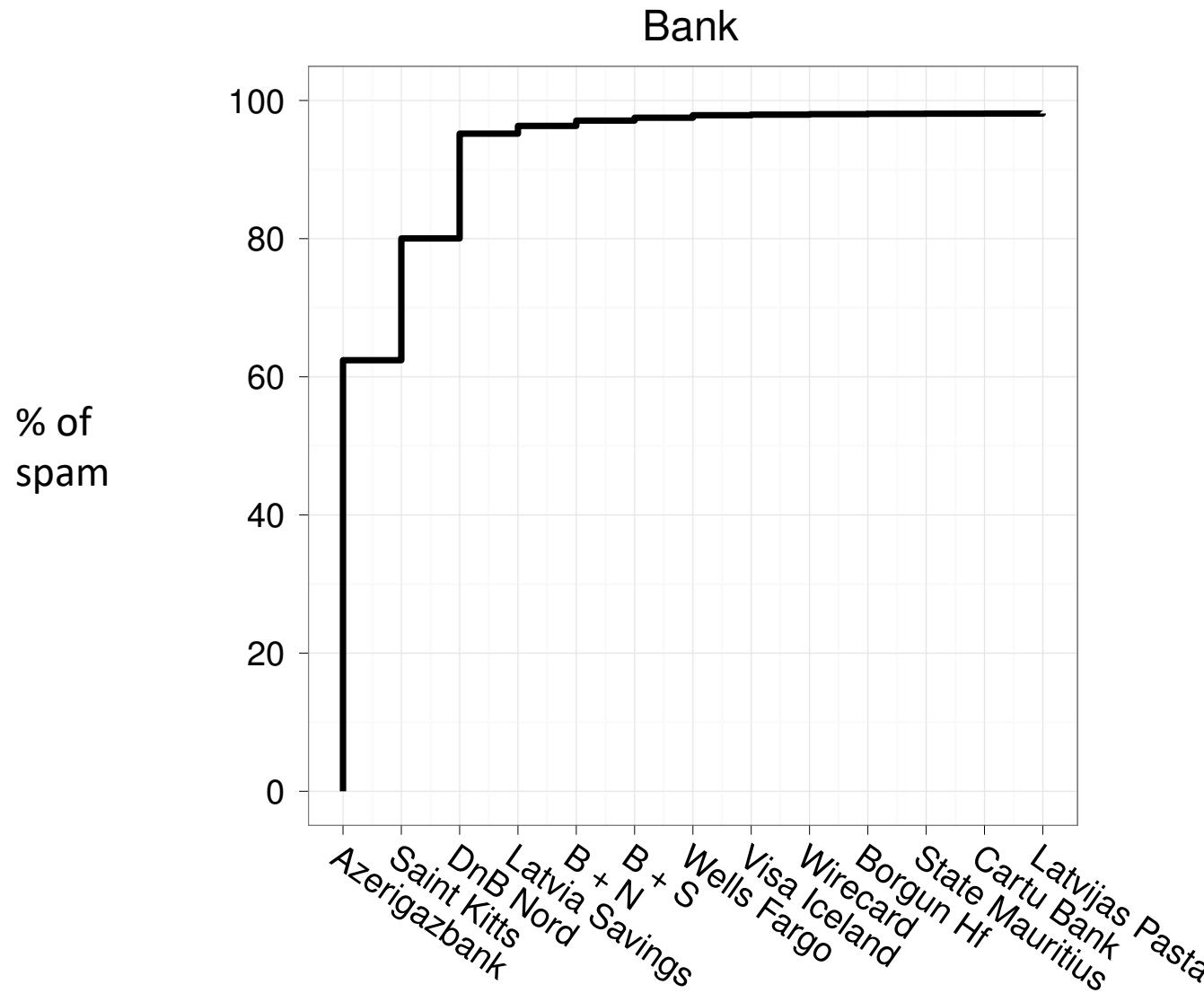


From Levchenko et al., "Click Trajectories: End-to-End Analysis of the Spam Value Chain", IEEE Symposium on Security and Privacy, 2011

- 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)

<i>Supplier</i>	<i>Item</i>	<i>Origin</i>	<i>Affiliate Programs</i>
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.



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

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 with Bot C&C servers

Publicly addressable bots advertise as able to C&C proxy

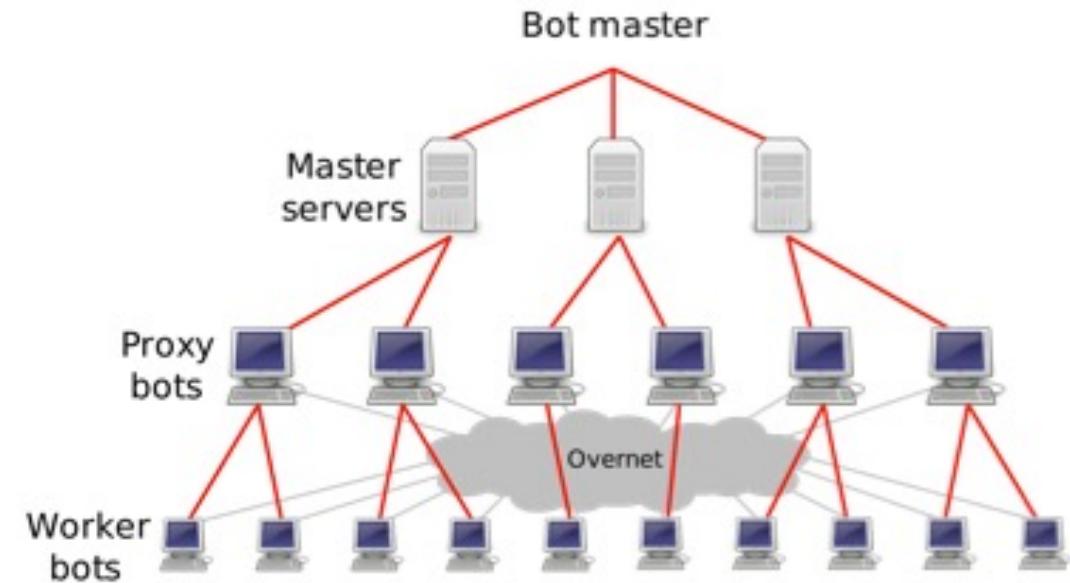


Figure 1: The Storm botnet hierarchy.

Fast-flux DNS

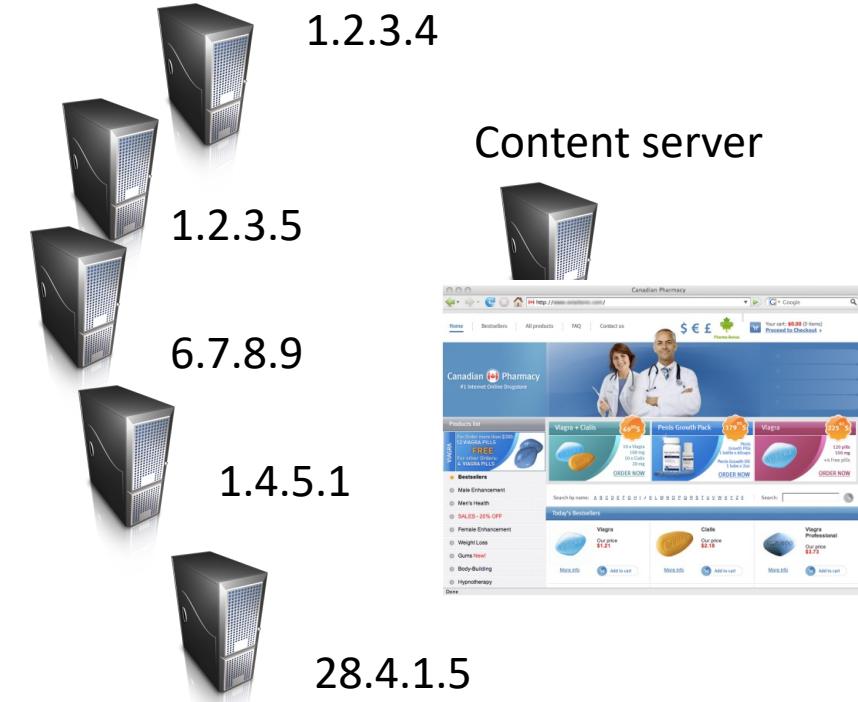
Spam campaign that directs users to ***pharmashop.com***

Single flux:

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

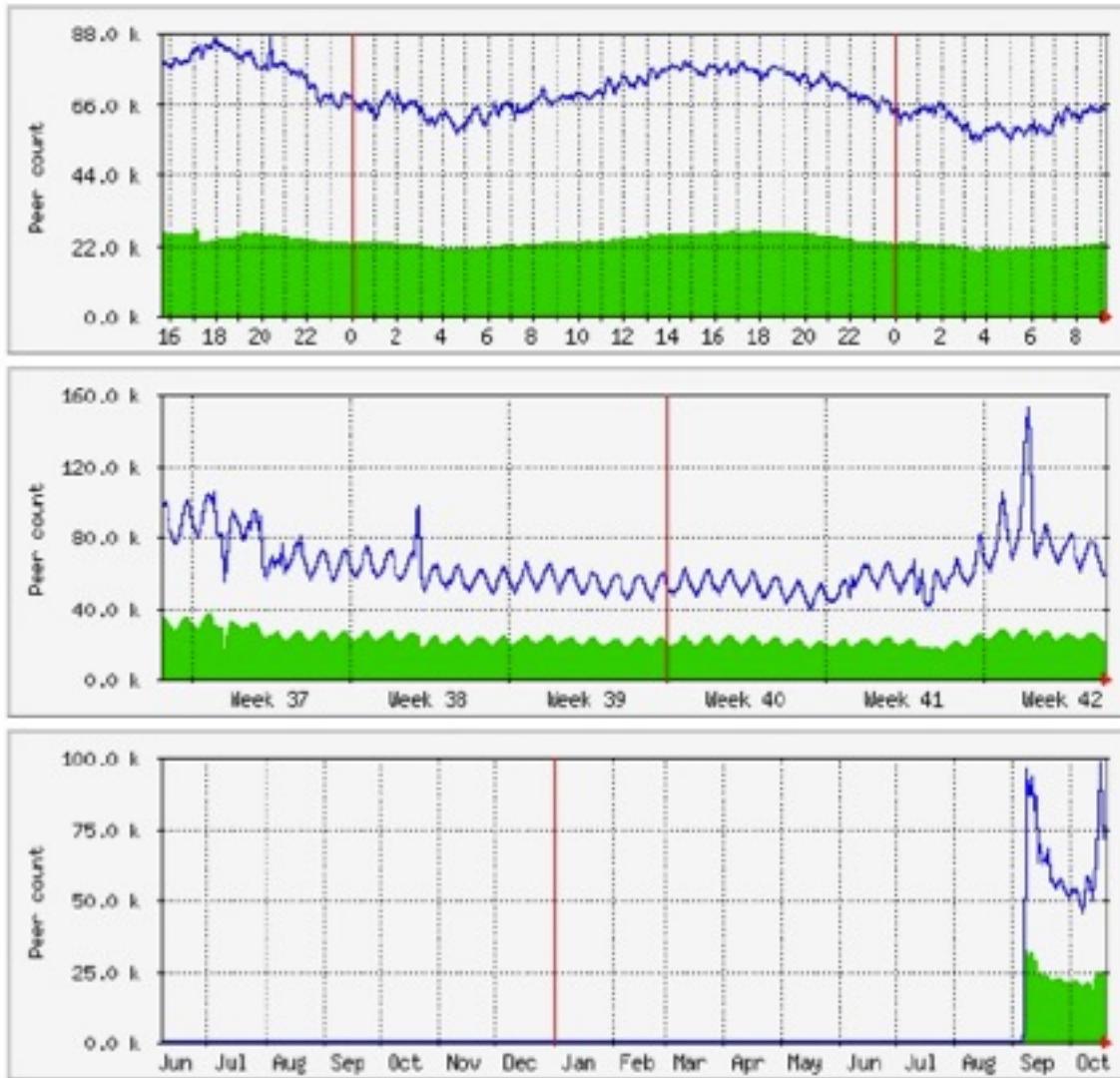
Double flux:

- 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 (Nuwarr) 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
```

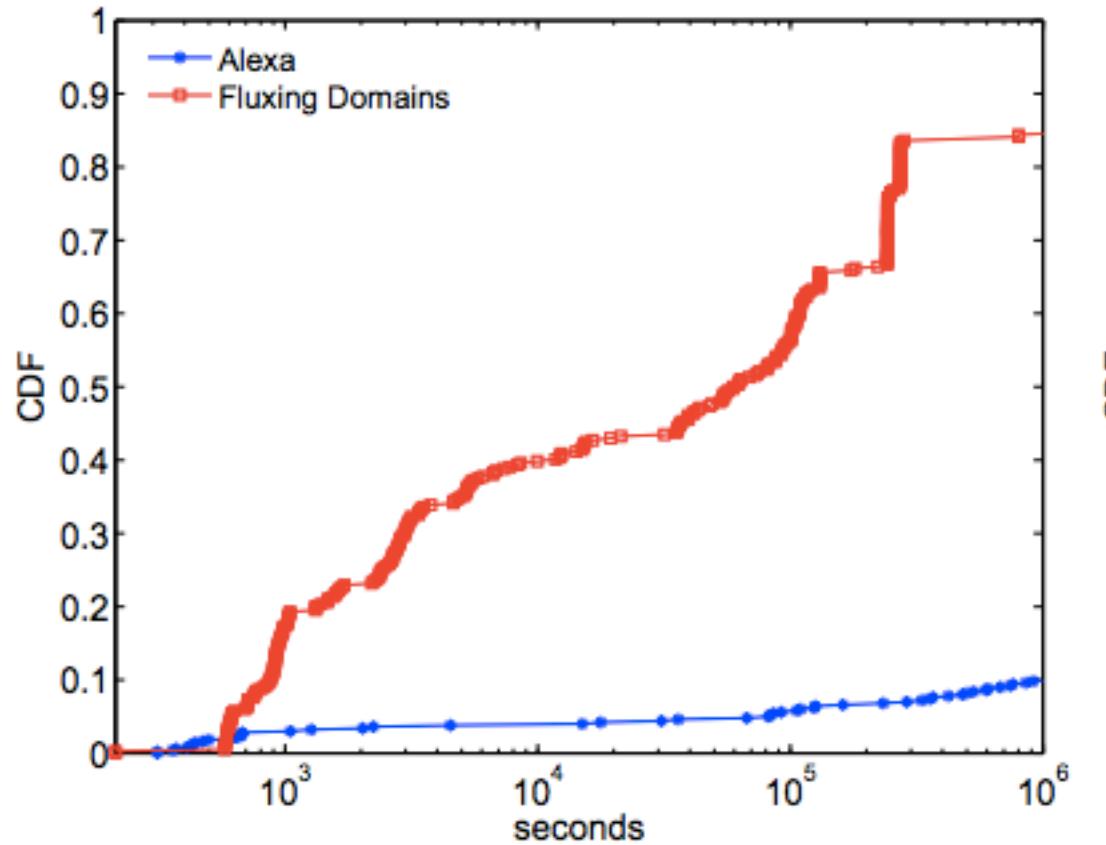
```
;; ANSWER SECTION:  
thearmynext.info. 600 IN A 213.47.148.82  
thearmynext.info. 600 IN A 213.91.251.16  
thearmynext.info. 600 IN A 69.183.207.99  
thearmynext.info. 600 IN A 91.148.168.92  
thearmynext.info. 600 IN A 195.38.60.79
```

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



Konte et al. 2008

<http://www.cc.gatech.edu/~fteamster/papers/fastflux-tr08.pdf>

(a) A records

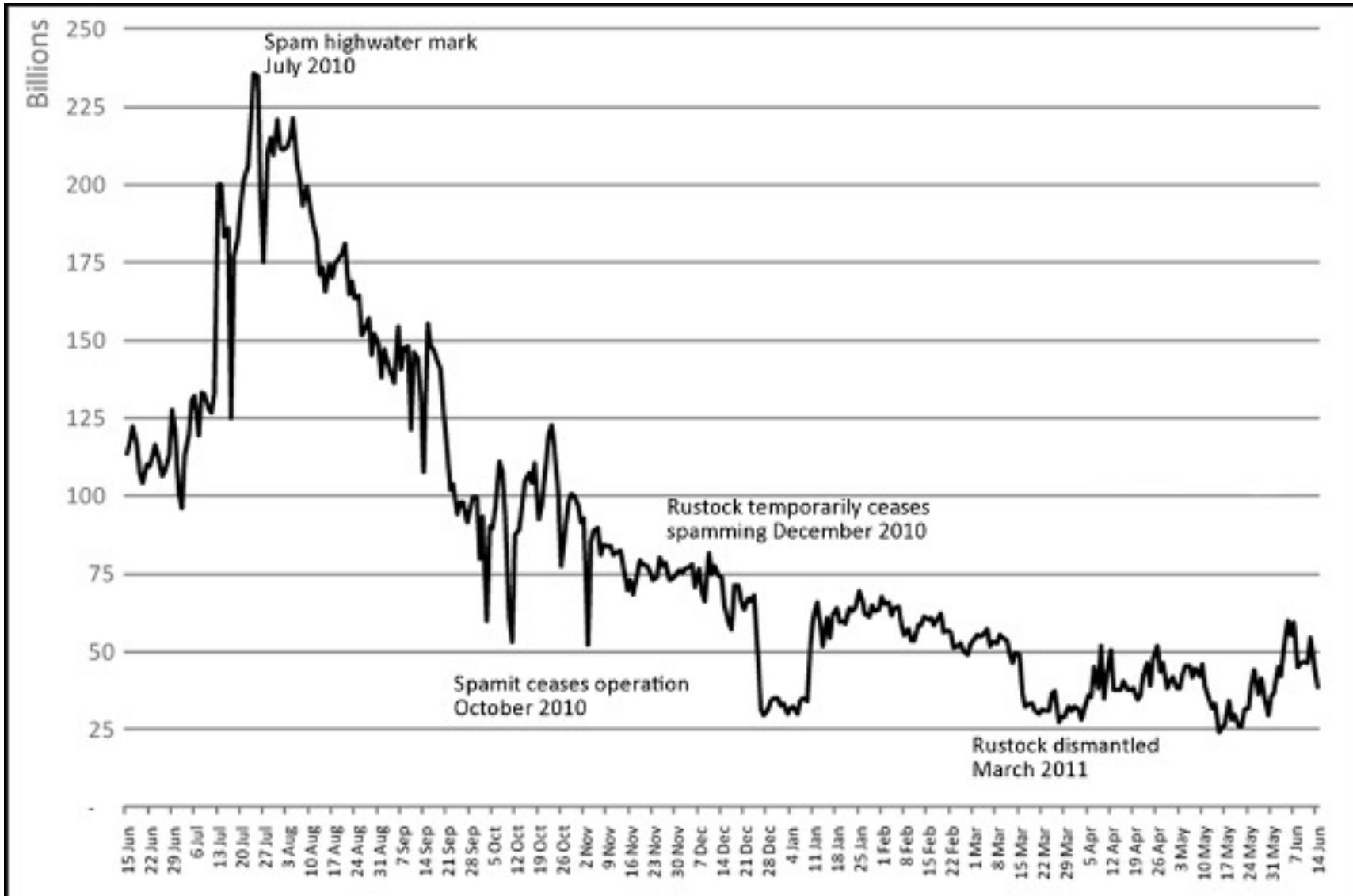
Studying fast-flux

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

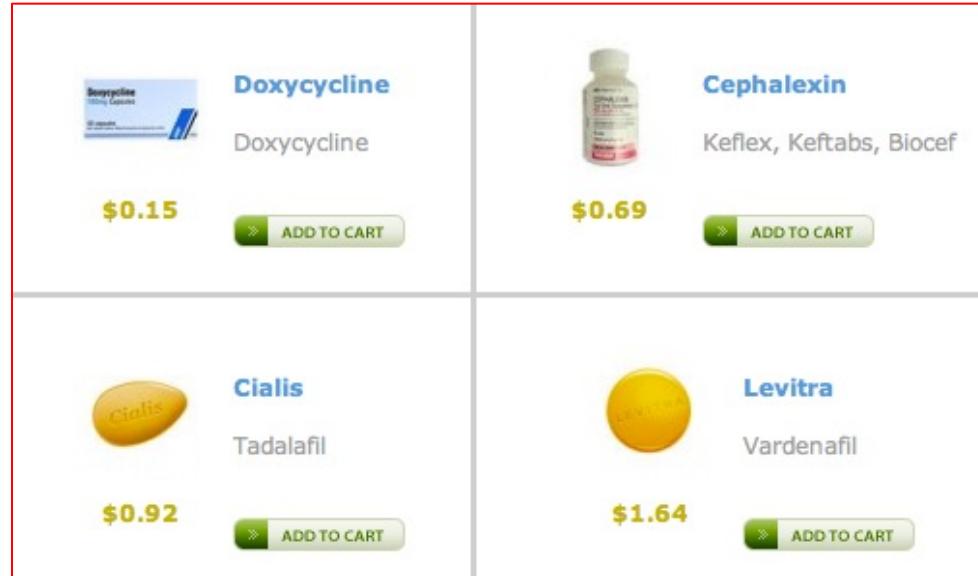
<https://media.blackhat.com/us-13/US-13-Xu-New-Trends-in-FastFlux-Networks-WP.pdf>



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

Spam-advertised products

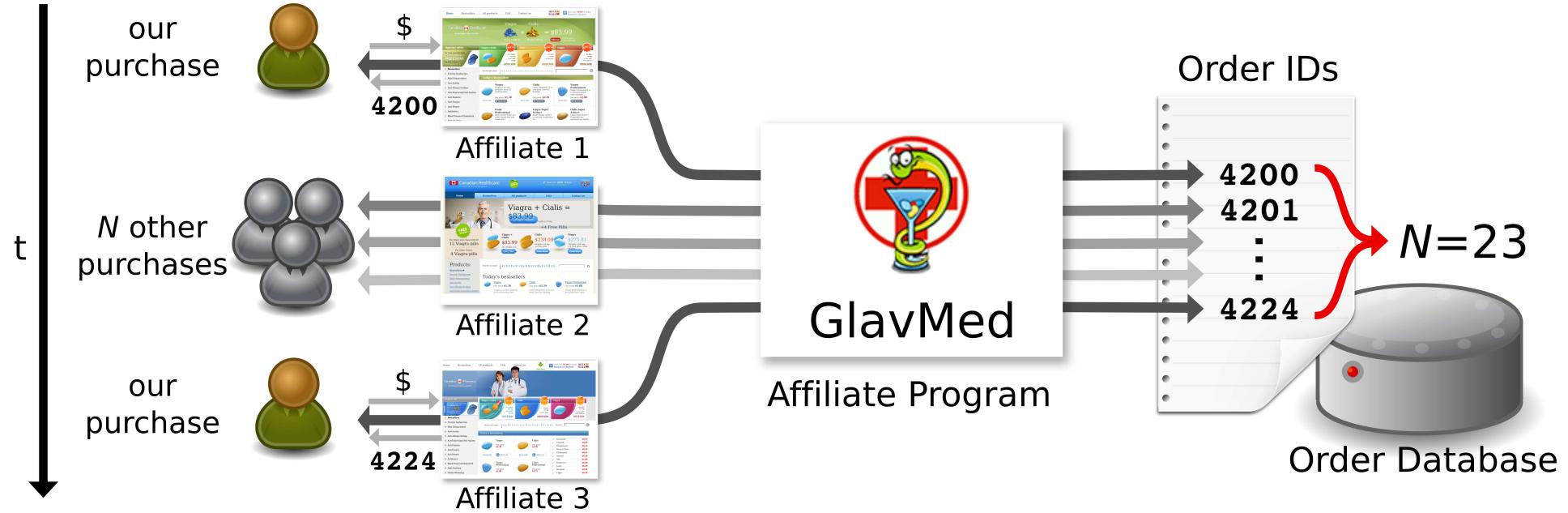
- Pharmaceuticals
- Software
- Watches
- etc.



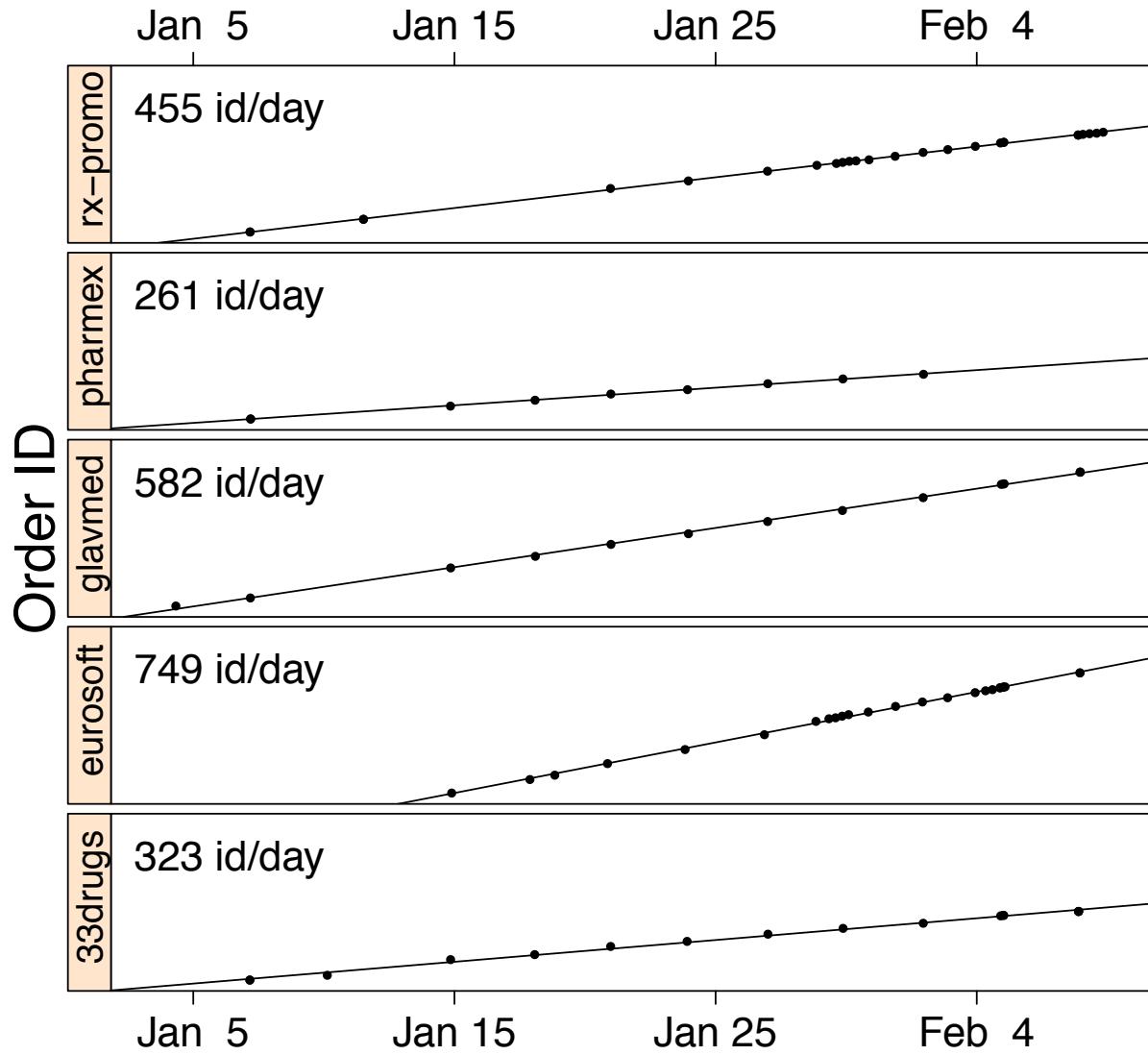
- What is order volume?
- What kinds of things are being purchased?
- What are weak links for disruption?

<http://www.rioricopharmacy.com/>

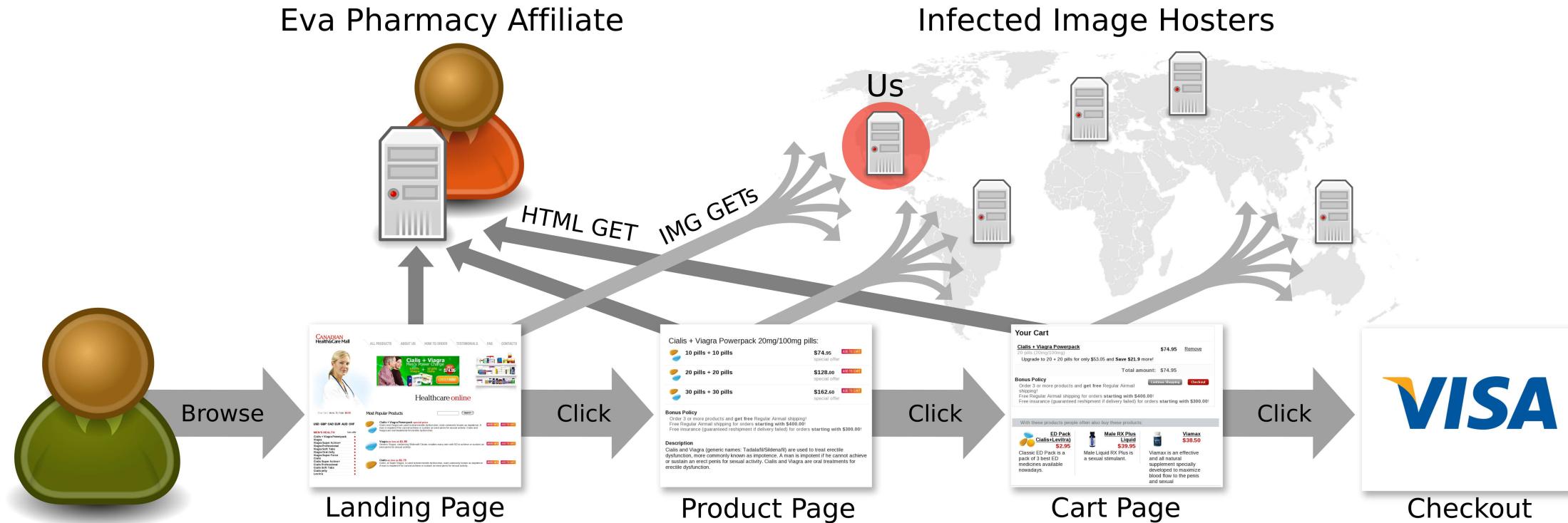
Measurement apparatus #1



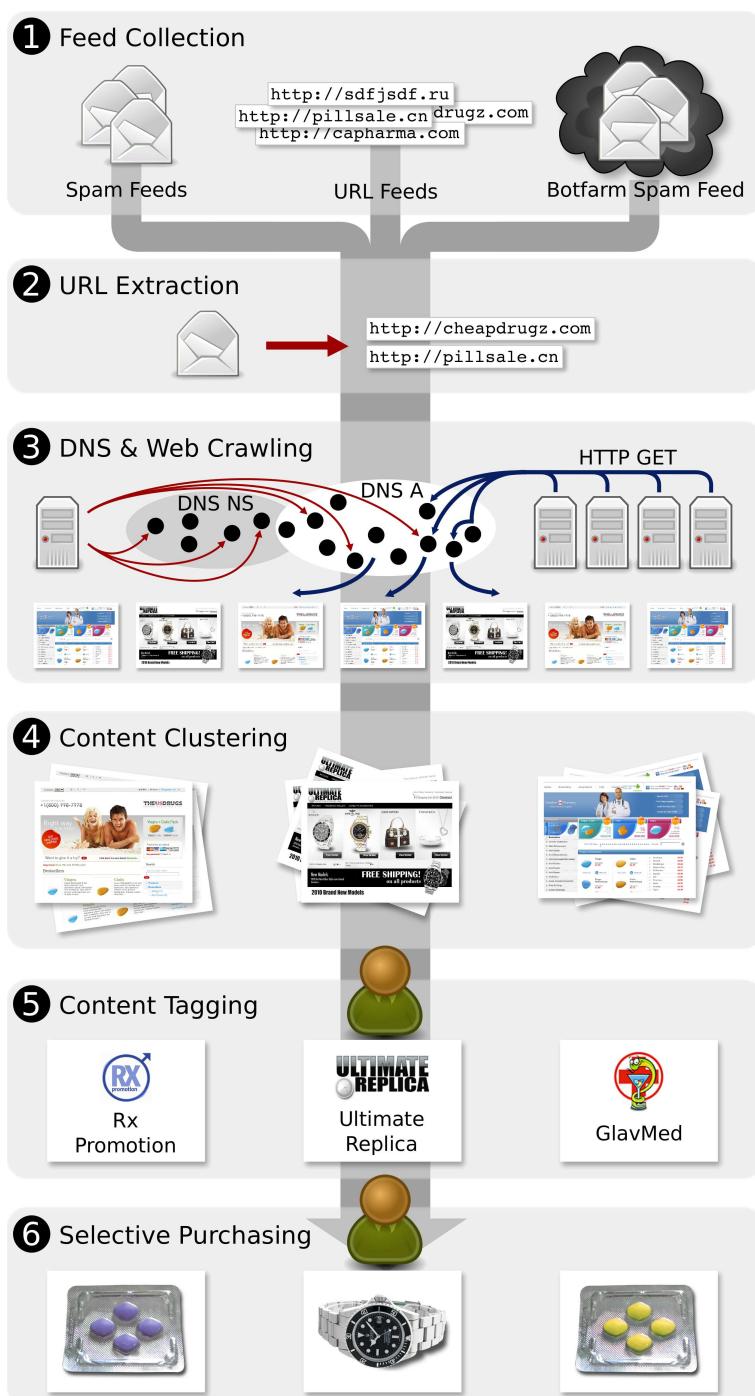
Kanich et al., Show Me the Money: Characterizing Spam-advertised Revenue, 2011



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



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