COMPUTER SCIENCE
& ENGINEERING
TEXAS A&M UNIVERSITY

Cybercrime in the Deep Web

Dr. Martin “Doc” Carlisle

Agenda

- **Overview of online crime**
- **Case studies**
  - Online sale of drug
  - How FBI shut down Silk Road
- **Ongoing cyber crime examples**
  - IRS tax returns
- **Give you an idea of**
  - Different players involved in online crime
  - Intervention strategies

Online crime

- **Emergence of underground economy**
  - Loose federation of specialists selling capabilities, services, and resources explicitly tailored to the abuse ecosystem
- **Streamlines abuse – for a fee**
  - Commoditization provides access to:
    - Compromised machinery
    - Sensitive user data
    - Human services
    - Accounts & engagement
  - Difficult for any single actor to extract all this value

Online crime – Profit centers

Flow of external capital into underground

Slide ack: Thomas Kurt

Online crime – Support centers

Specialized Payloads	**Spambot** *Grum, Storm, MegaD*	**Clickbots** *ZeroAccess*	**Banking trojans** *Zeus, SpyEye*
Malware distribution	**Exploit kits** *Nuclear, Blackhole*	**PPI services** *GoldInstalls, Loader Adv*	--
Traffic acquisition	**Accounts** *Email, social, phishing*	**SEO, cloaking** *Backlinks, websites*	--
Raw materials	**Hosting, networking** *Hosts, proxies, domains*	**Human services** *Captcha, SMS, content, mules*	--

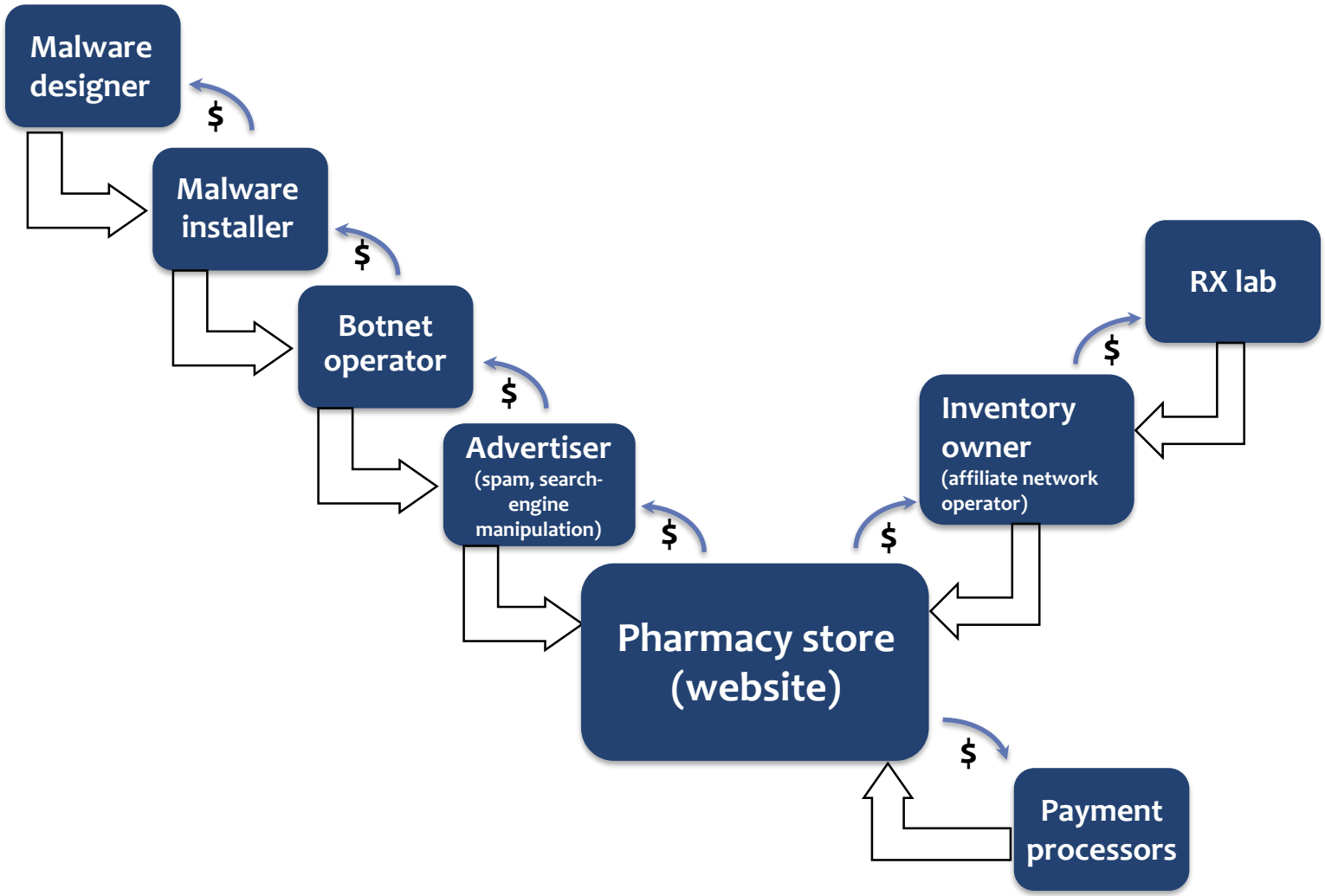
Flow of capital into underground

Slide ack: Thomas Kurt

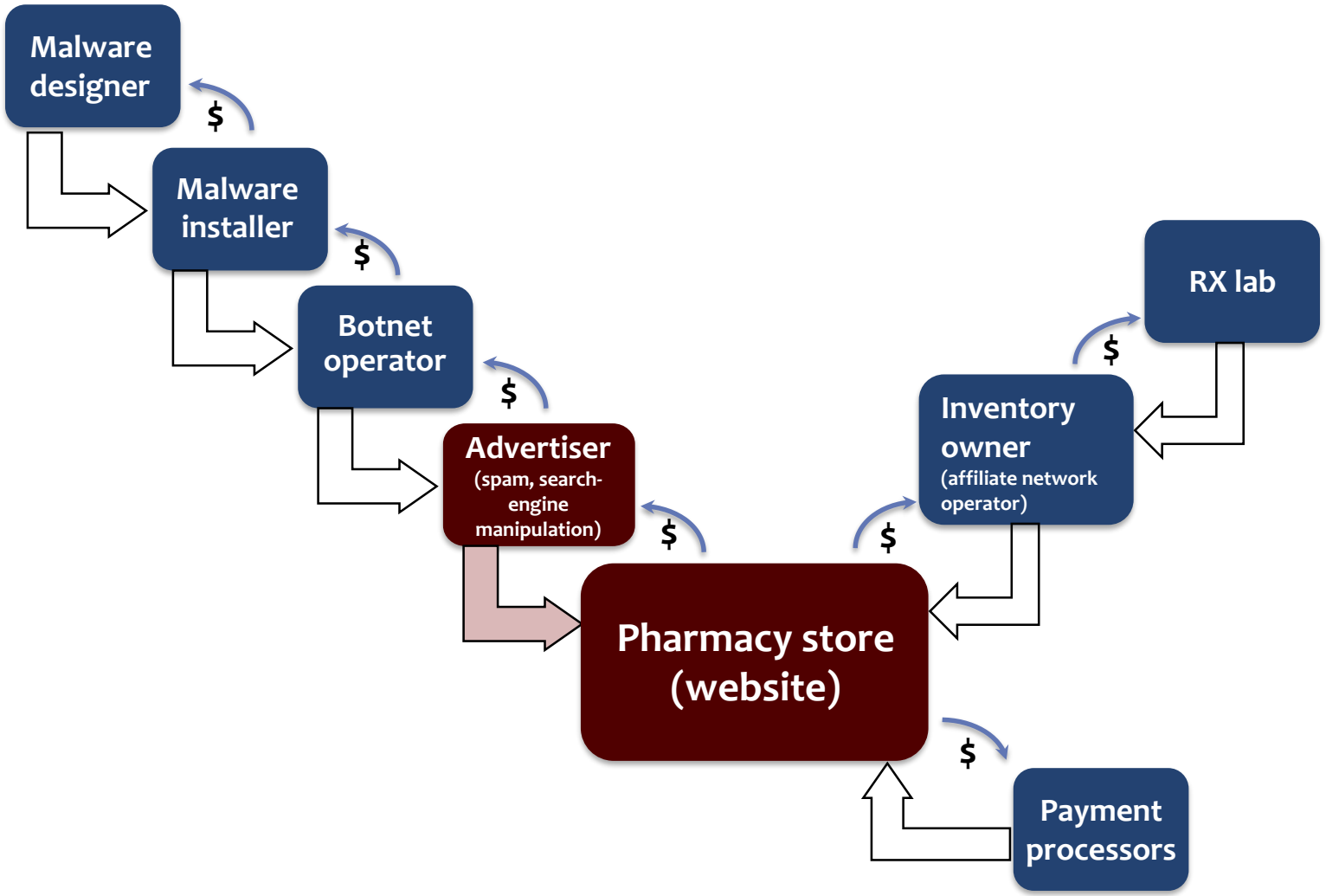
Case study: Online sale of drugs

- **One of the best known illicit online trades**
  - Who hasn't received email spam for prescription drugs?
- **Potentially most dangerous form of online crime**
  - Wrong dosage can kill: cf. Ryan Haight
- **Complex supply chain that can tell us a lot about the online criminal ecosystem**

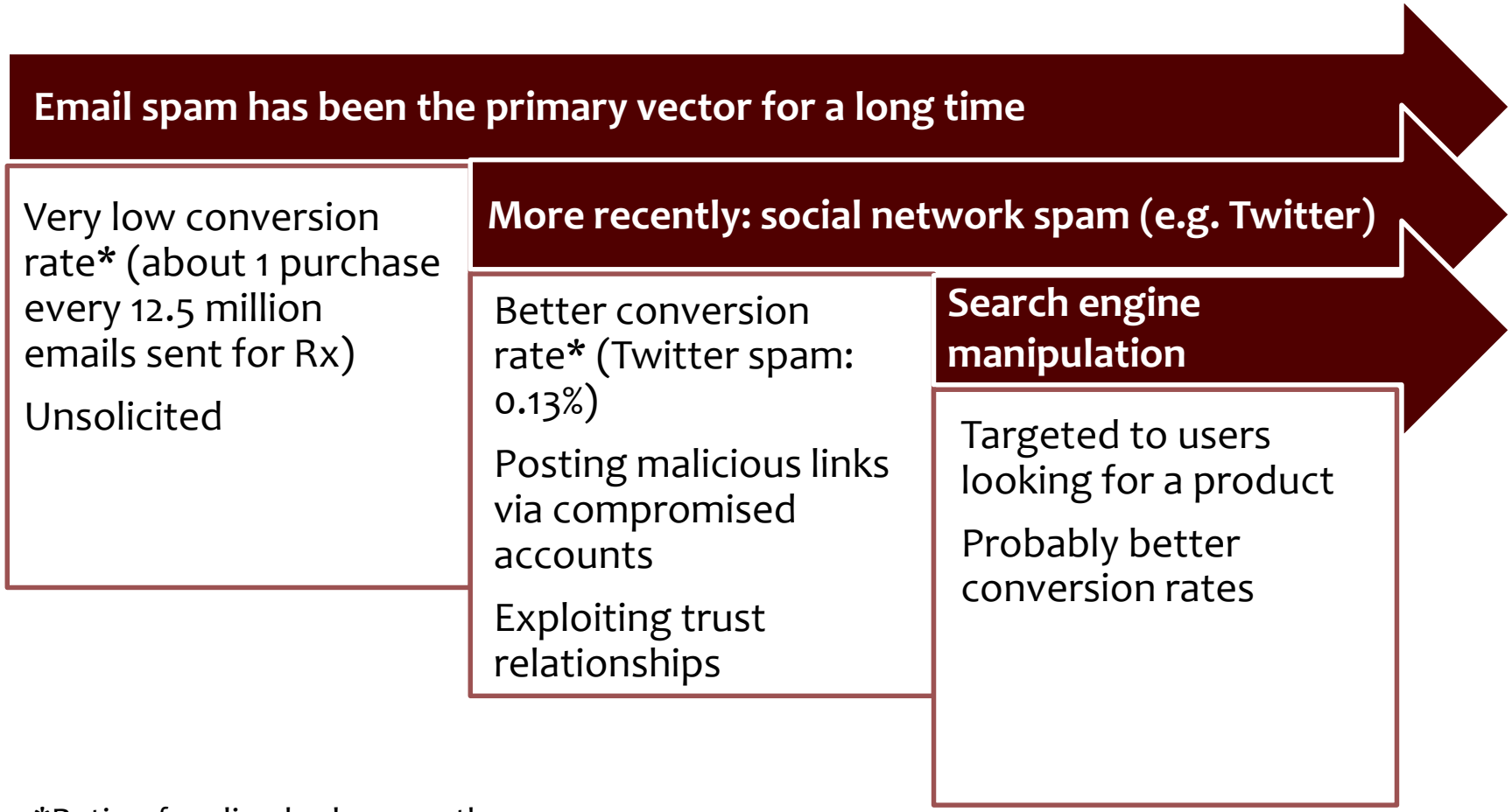
Supply chain: high-level overview



Advertising unlicensed drugs



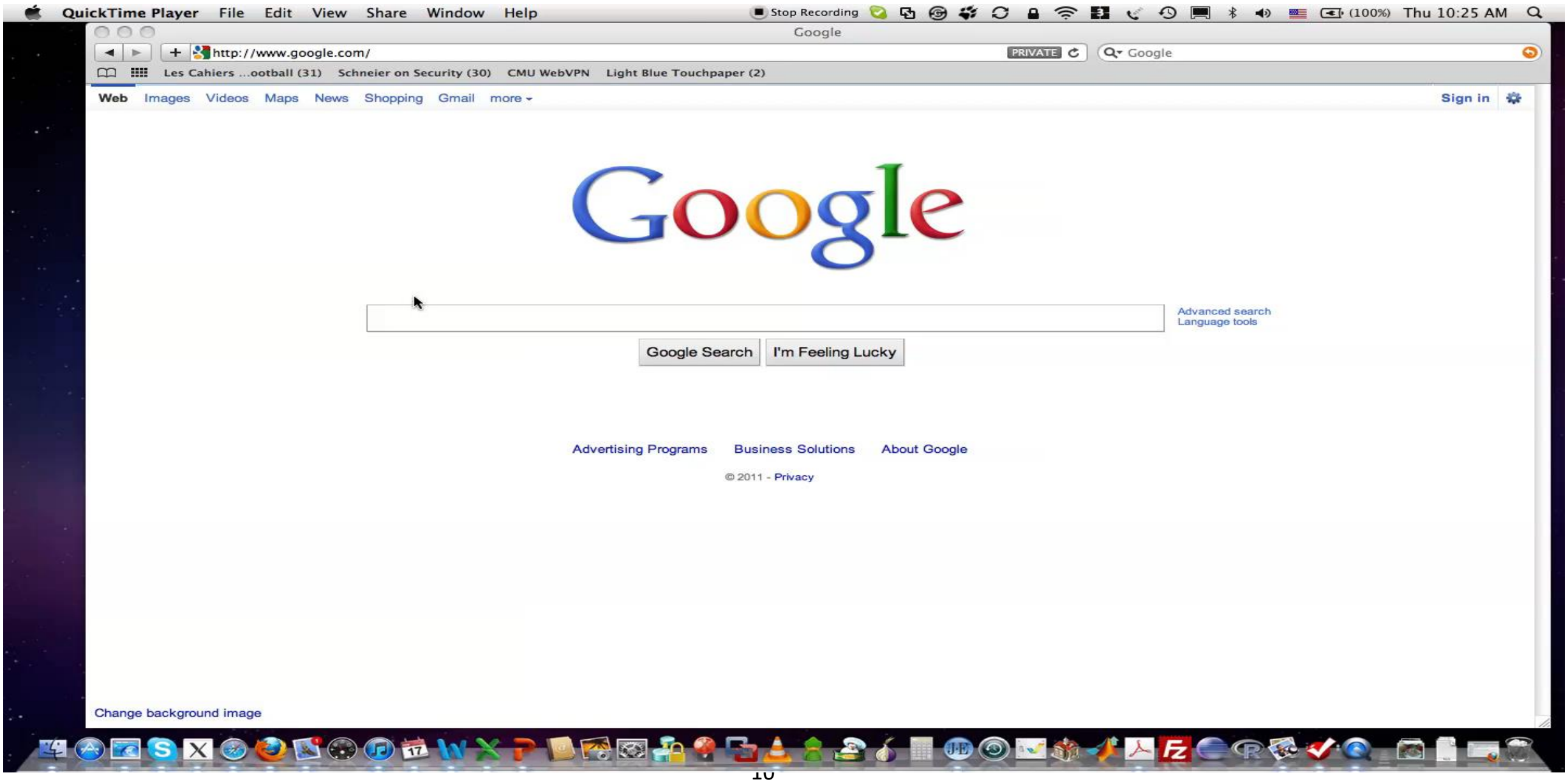
Evolution of advertising of illicit products



*Ratio of realized sales over the number of emails/clicks

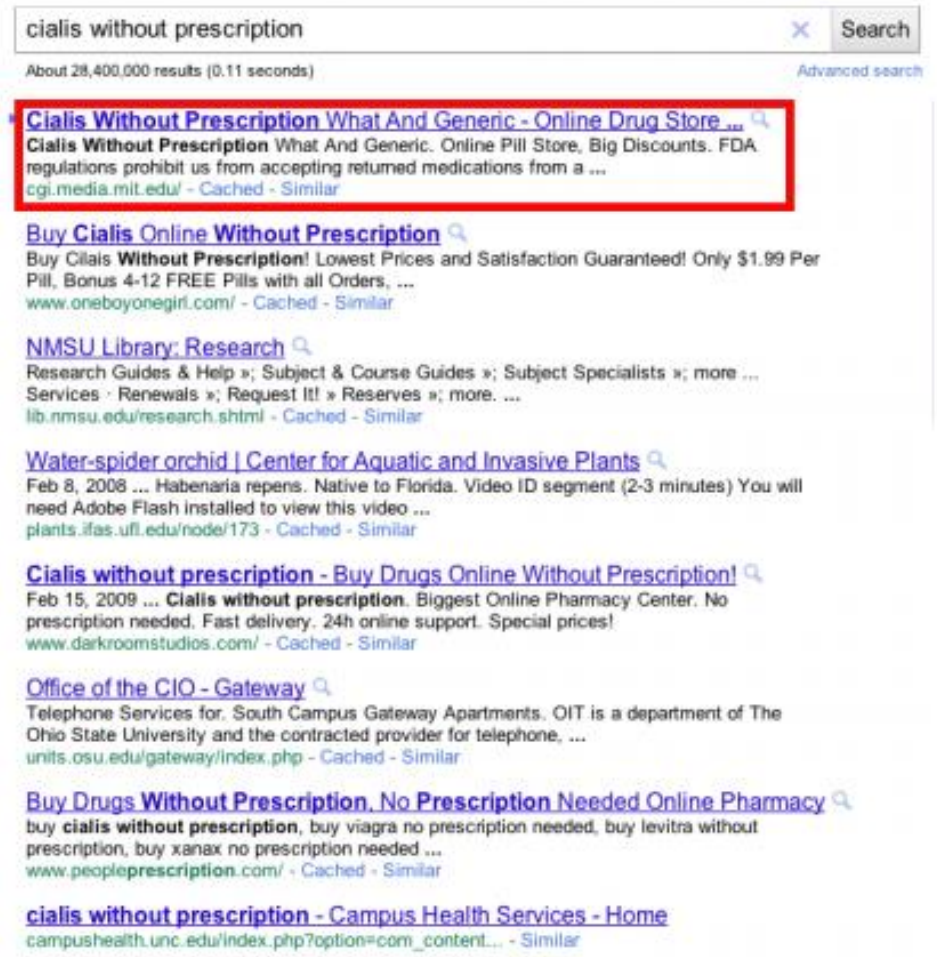
Original search-redirection attack (1)

[Leontiadis, Moore and Christin, USENIX Security 2011]



Original search-redirection attack (2)

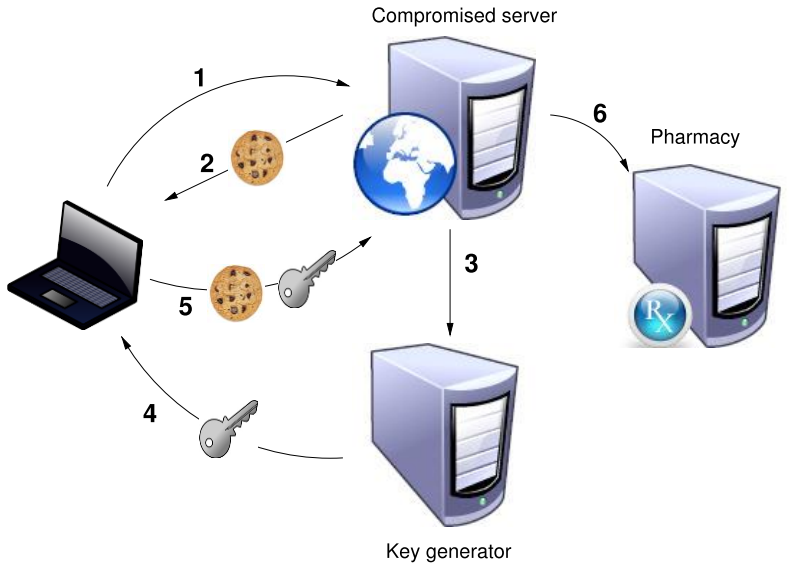
[Leontiadis, Moore and Christin, USENIX Security 2011]



Only **two** of the results actually belong to online pharmacies. The rest are unrelated .com or .edu sites that had been compromised to redirect to online pharmacies or have been populated with spam.

Novel attack variants (2012+)

- **Ex.1 Inlining the store front in the compromised website**
  - A click then leads you to the pharma store
- **Ex.2 Stateful server**
- **Goal: escape detection by automated crawlers**

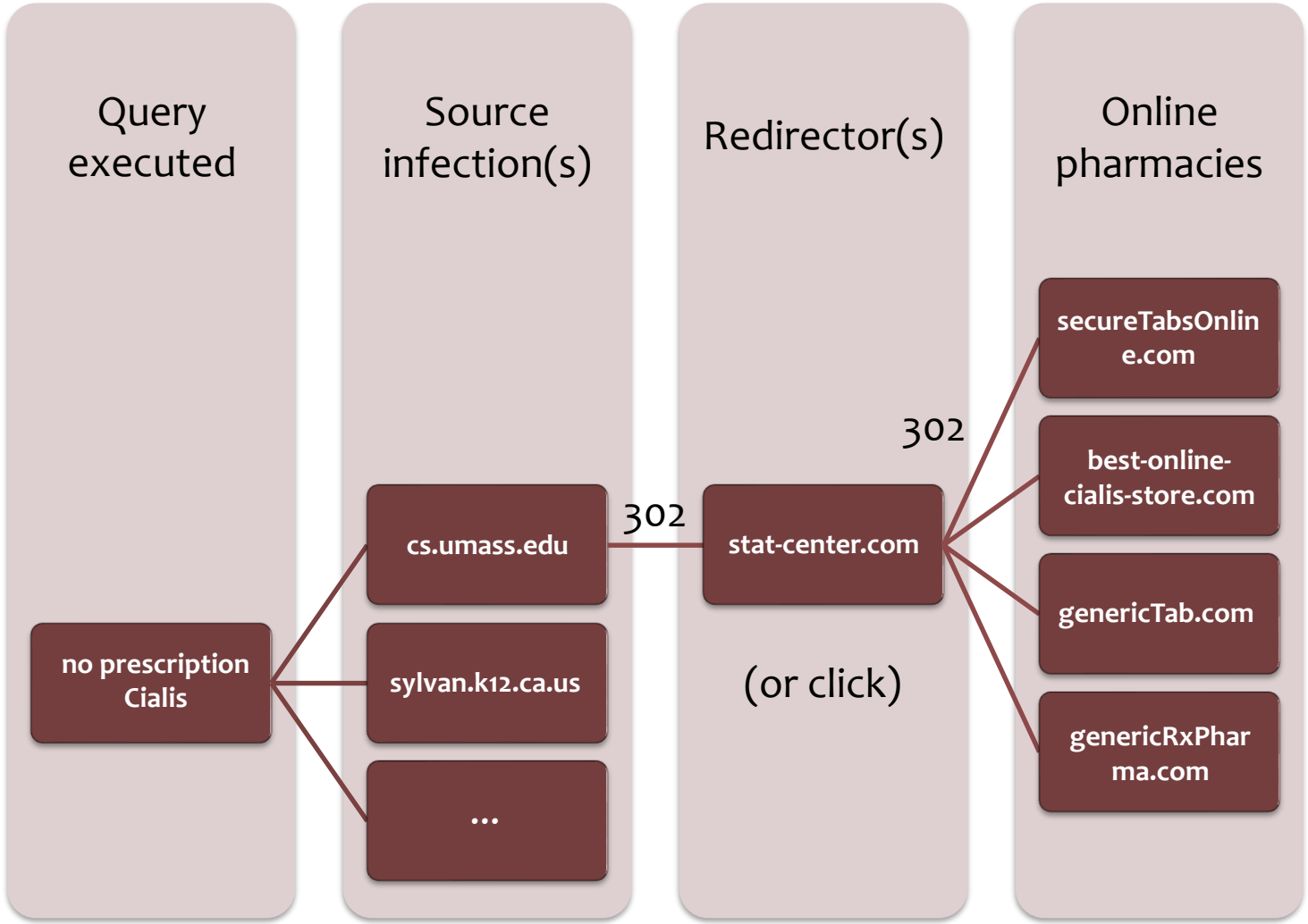


- Attackers are quickly adapting to monitoring and/or countermeasures
- Non-trivial amount of effort on their part!

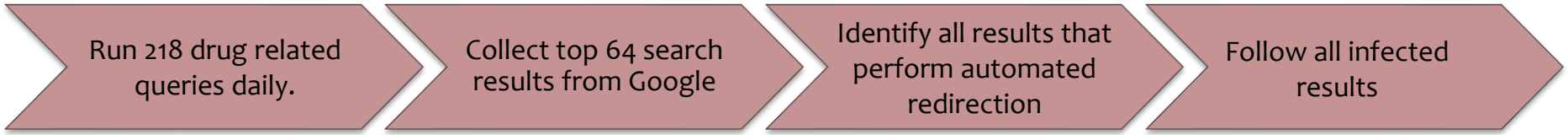
Questions

- **How has the attack evolved?**
  - Volume and impact
  - Techniques
- **Why has the attack evolved?**
  - Effectiveness of the defenses?
- **Can this be thwarted?**
  - Network-level intervention vs. end-host intervention

Attack modus operandi: Redirection chains



Data collection process



- Daily collection from 4/12/2010 through 9/16/2013

- The limit is defined by Google Search API
- Storing all results for later processing
- Will also examine position information

- A search result defines the website that a user will be redirected to when clicking on the link
- If the browser is redirected instead to a different website (domain), the result is infected.

- Follow each result identified as infected from previous step
- Follow all redirections that might occur
- Record all the redirection information

Datasets collected

[Leontiadis, Moore and Christin, ACM CCS 2014]

- **Dataset 1**
  - Aggregate results only
  - Rank of the results unknown
  - Mapping query-results unknown
- **Dataset 2**
  - Same as Dataset 1, but ranking information known
  - Mapping query-result doesn't include rank
- **Dataset 3**
  - All information is captured
  - … but Google started to limit what we could get

Dataset	1	2	3
Period	4/12/10-11/15/10	11/15/10-10/8/11	10/8/11-9/16/13
Search results/query	64	64	16/32
Total results	260,824	3,609,675	1,530,099
Unique URLs	150,955	189,023	122,382
Unique domains	25,182	36,557	30,881

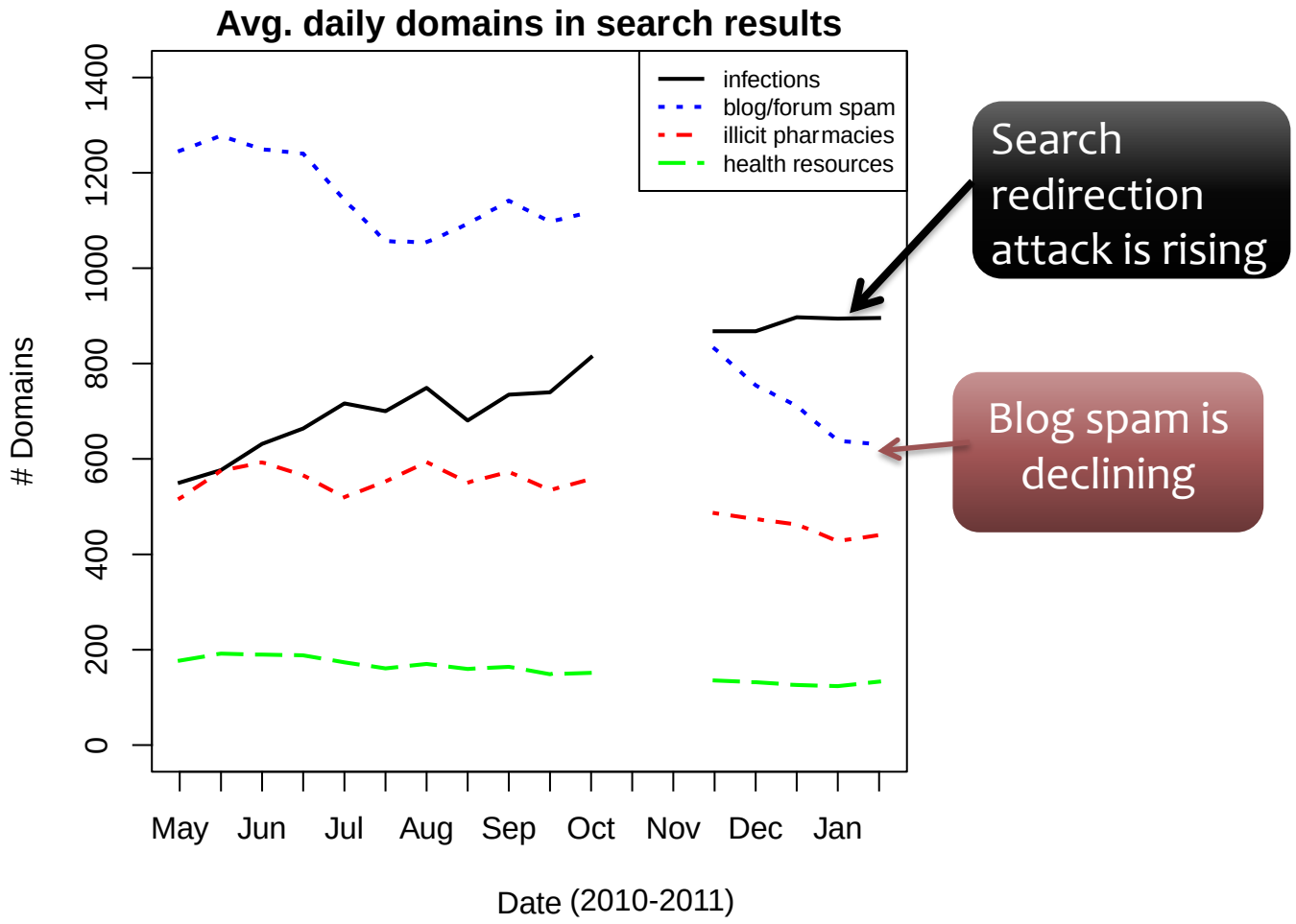
Some of the 218 queries used

vicodin no prescription
cheap valium non prescription
buy ativan online injecting pills
buy xanax valium online florida
order vicodin si levitra online
buy xanax valium online florida
color of adipex pills safest place to buy online
vicodin without prescription
generic cialis free sample
cheap tadalafil
20 mg ambien overdose
prozac side effects
ambien buy online
alprazolam online without prescription buy cheap

Type	Count	Percent
Malicious (Black)	26	22%
Benign (White)	75	34%
Ambiguous (Gray)	117	54%
Total	**218**	**100%**

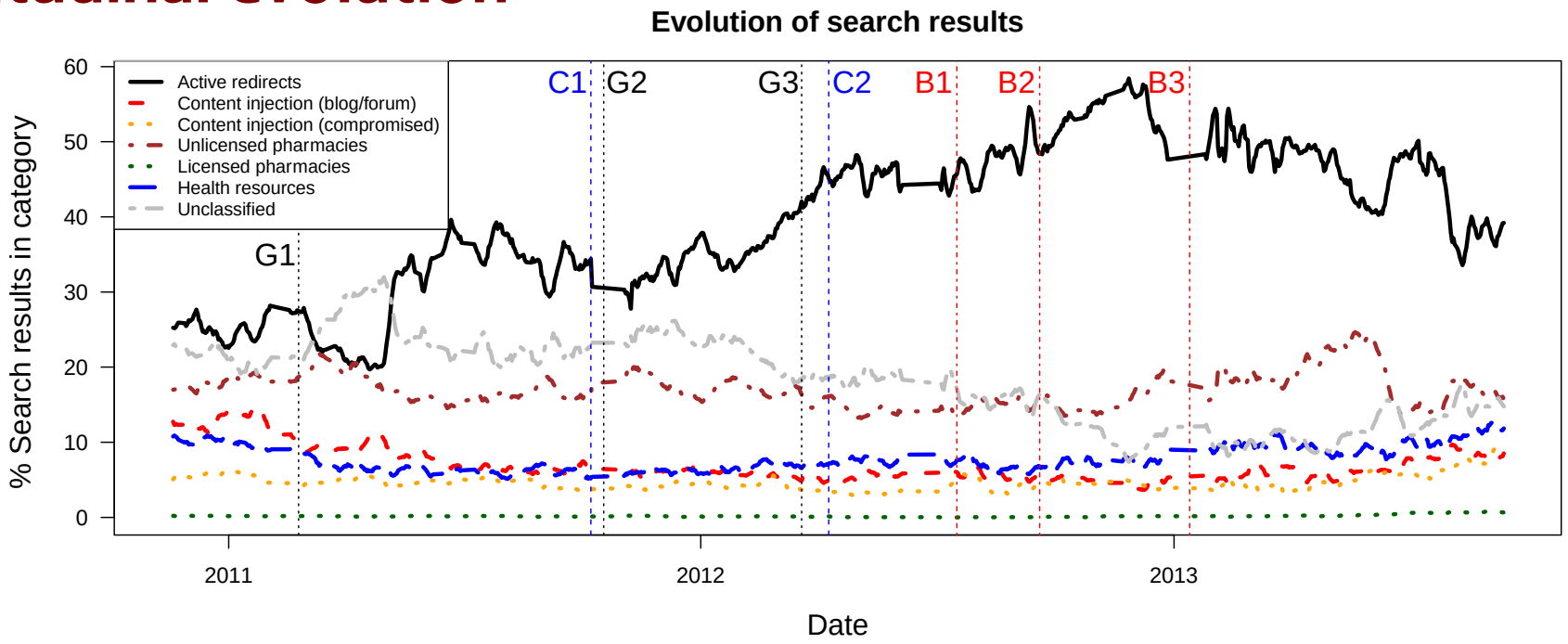
Dataset 1: 2010-2011

Search-redirection took over forum spam



Datasets 2: 2011-2013

Longitudinal evolution



G1: Google changes search ranking algorithm

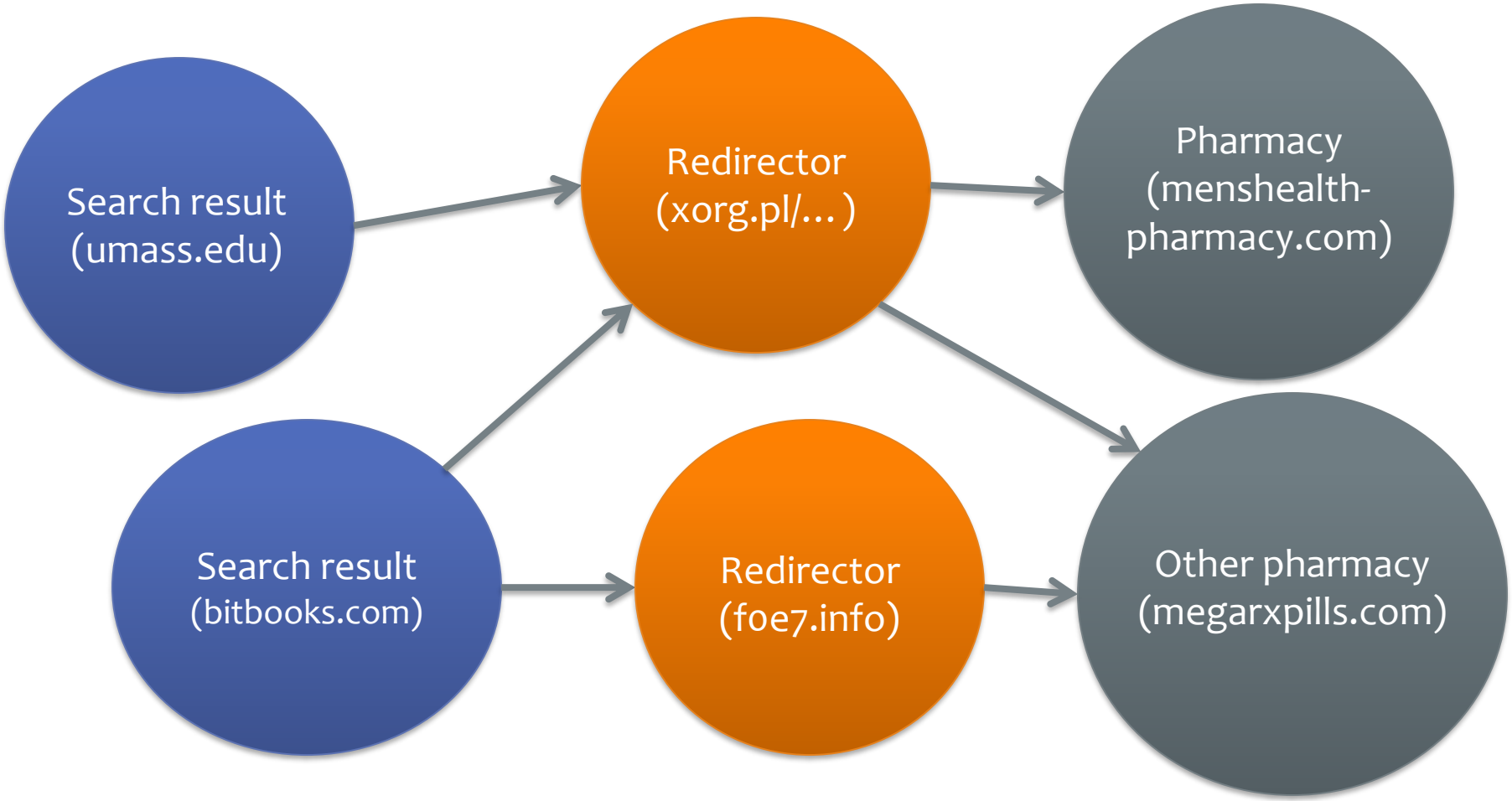
G2: Google starts removing query info from "Referer" field

G3: Google is done deploying Referer modifications

B1, B2, B3 : Firefox, Safari, Chrome switch to HTTPS-only search

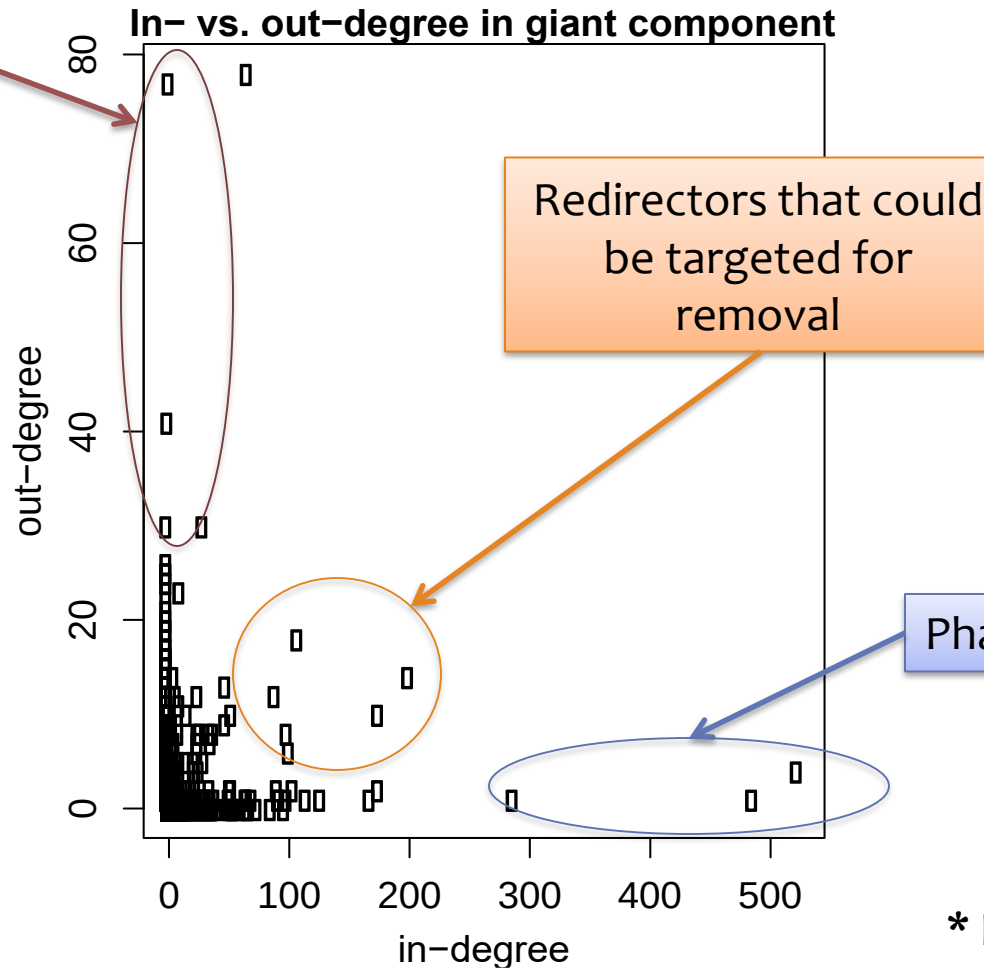
(C1,C2: major changes to our collection infrastructure)

Uncovering relationships in search results



Possible interventions (network side)

Valuable infected sites (e.g., umass.edu)

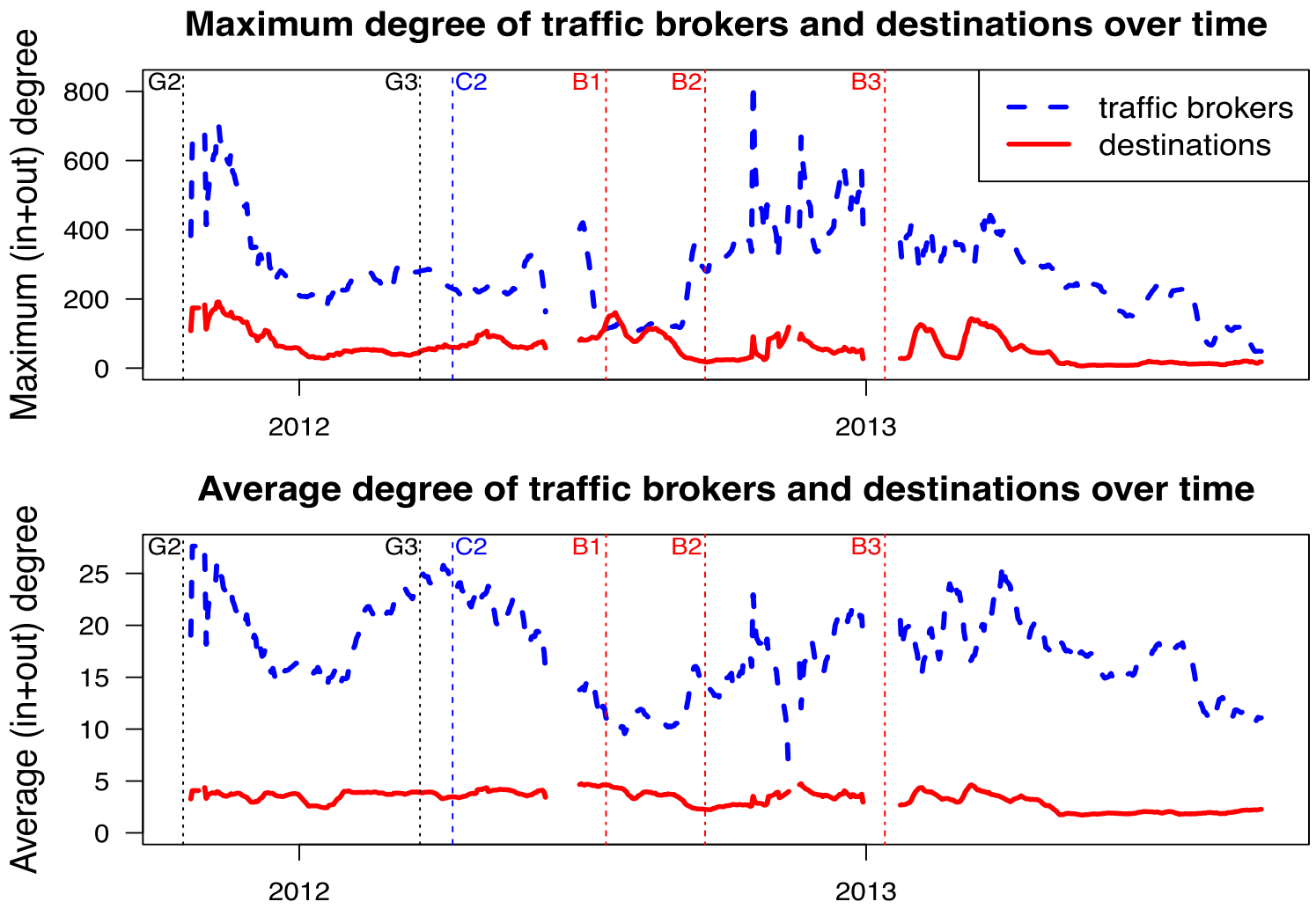


Redirectors that could be targeted for removal

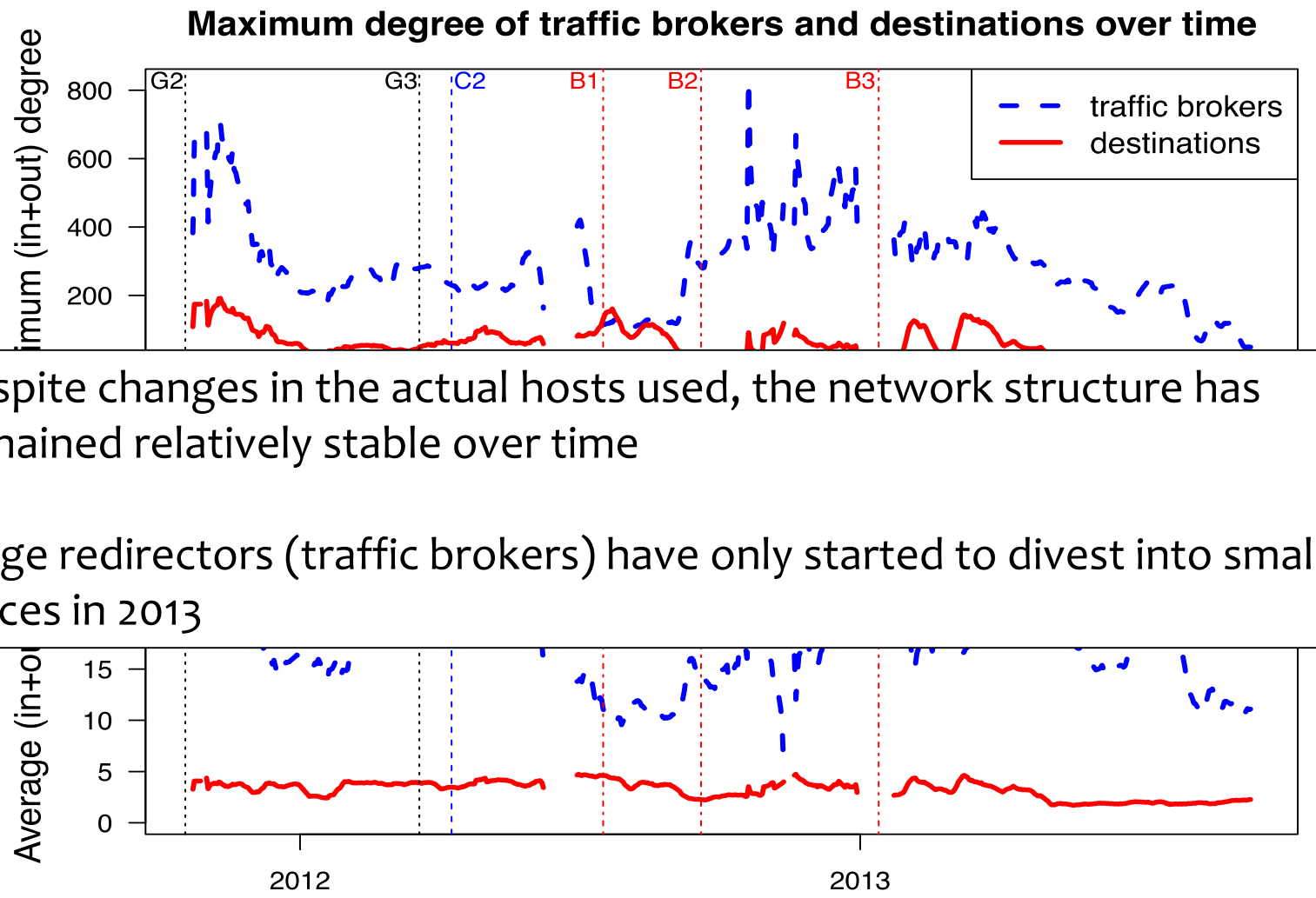
Pharmacies

*** Results here are for 2010-2011**

Evolution in concentration (1)



Evolution in concentration (2)

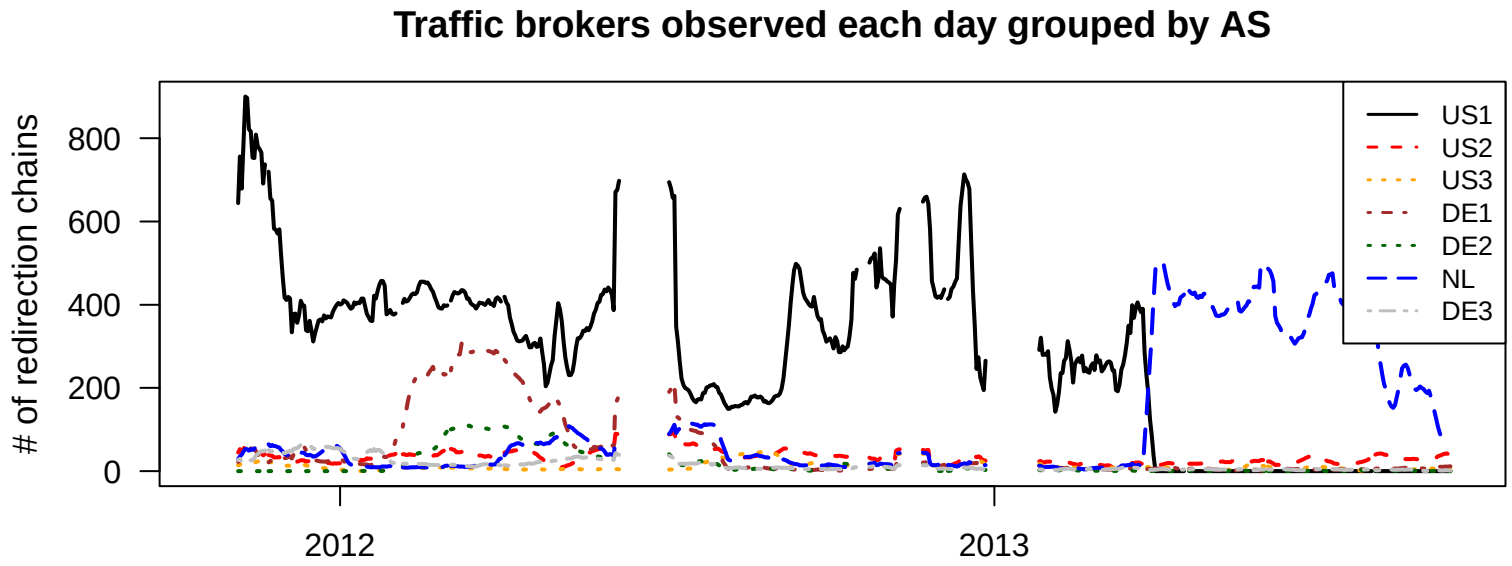


Despite changes in the actual hosts used, the network structure has remained relatively stable over time

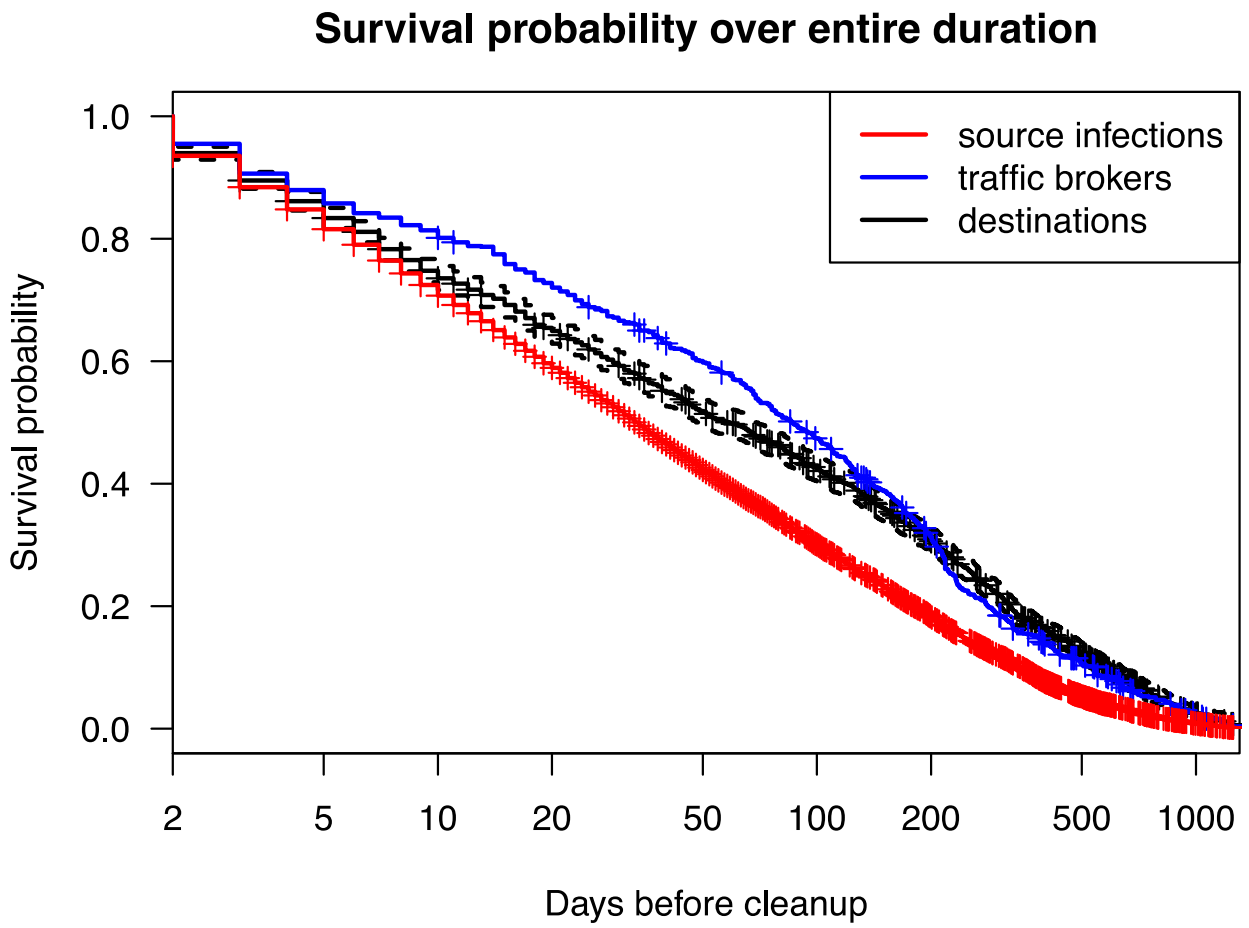
Large redirectors (traffic brokers) have only started to divest into smaller pieces in 2013

Network infrastructure used by illicit advertisers

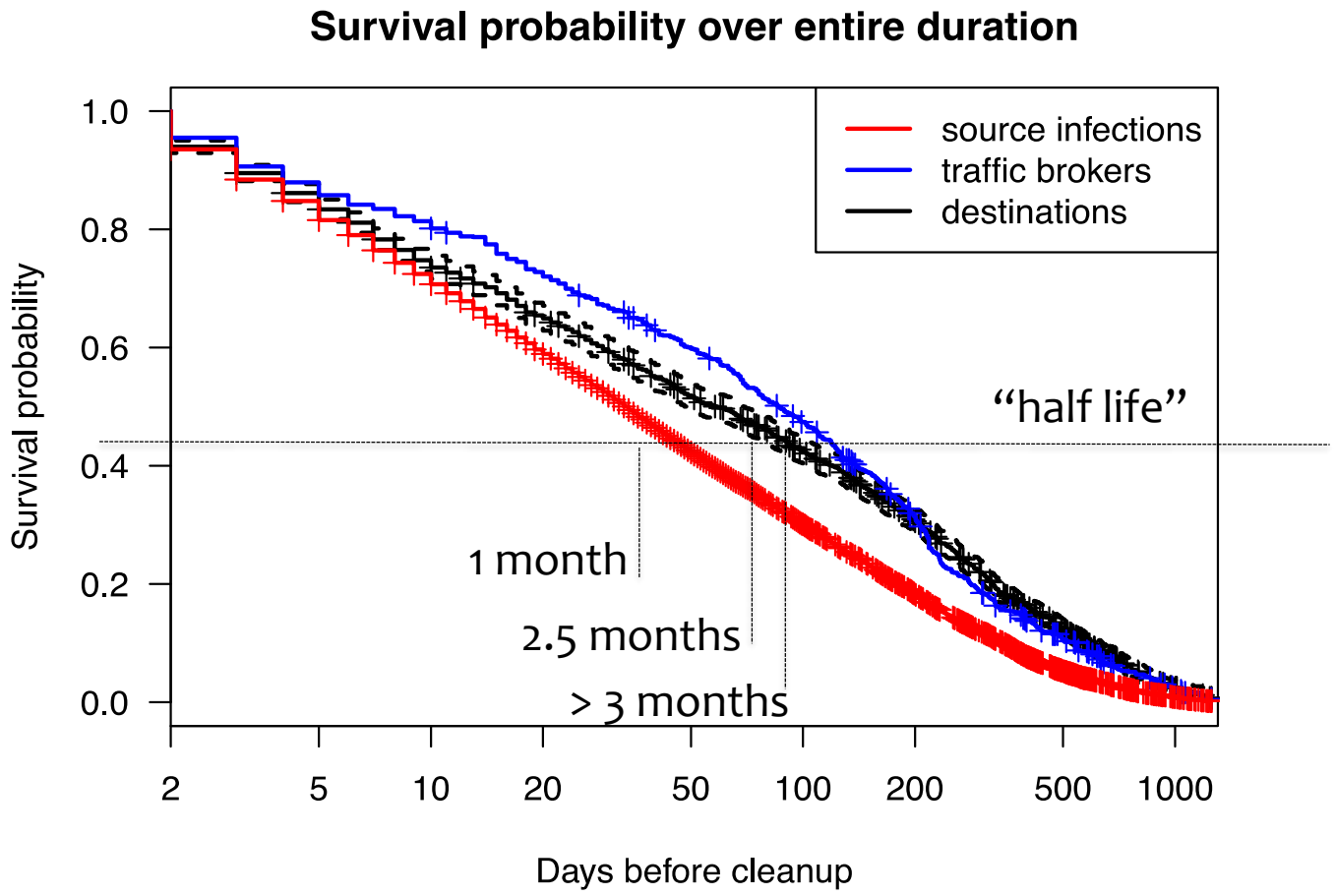
- Observed high concentration in traffic brokers
- Where are they located?



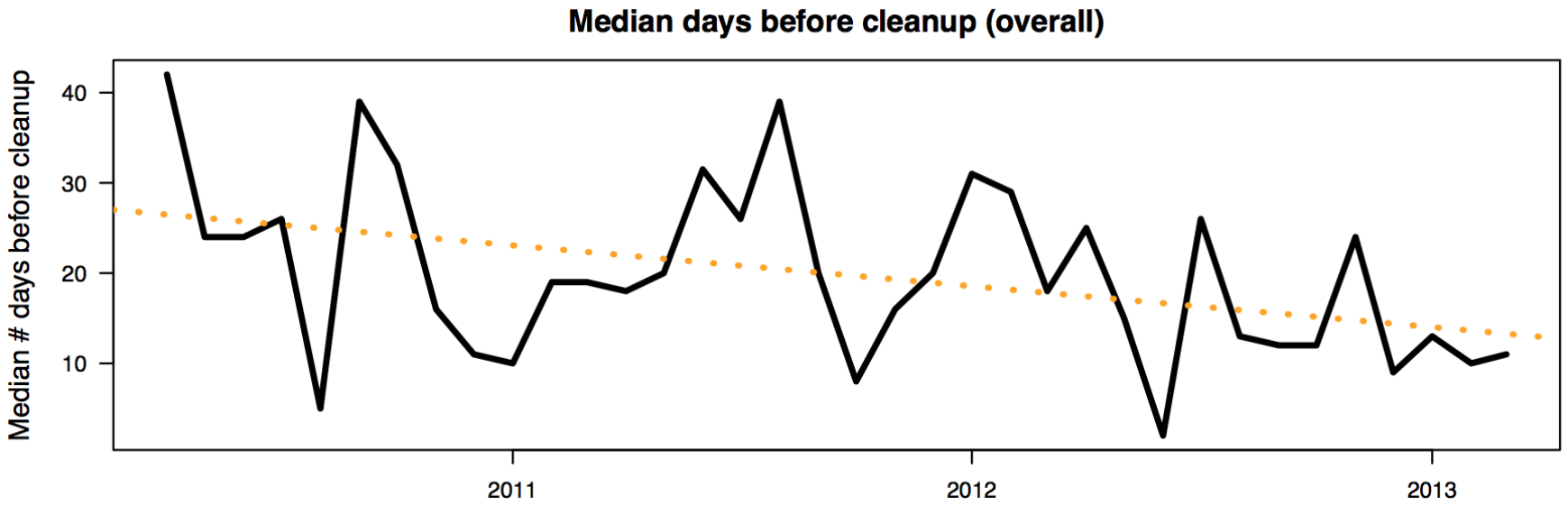
Effects of clean-up efforts (1)



Effects of clean-up efforts (2)



Effects of clean-up efforts (source infections over time)



Summary of measurement findings

- **Search-result poisoning is here and has become a primary vector of advertisement**
- **Four-year longitudinal study shows**
  - Little sign of abatement despite opportunities
    - Large concentration in traffic brokers, especially AS-level
  - Adaptivity of attackers to countermeasures
  - Clean-up time decreased at end-hosts but still large (1 month on average, still ~2 weeks+ in 2013)

Online criminal market place

- **A lot of dark market places**
  - Silk Road
  - Agora
  - Utopia
  - TheRealDeal
  - Alpha bay
  - …
- **Early adopters of technology**
  - Tor hidden service
  - Bitcoin

Silk Road—Beginning

- **Jan 1, 2011**
  An unknown individual using the alias 'altoid' begins posting on internet forums shroomery.org and bitcointalk.org, advertising a hidden Tor service like an "anonymous amazon.com."
- **March 1, 2011**
  Messages on Bitcoin Talk: Silk Road has been operational for 3 weeks
- **April 11, 2011**
  Silk Road hits 1000 users

Silk Road—Trails (1)

- **Oct. 11, 2011: Altoid Looks For a Bitcoin IT Pro**
  Bitcoin Talk user 'altoid' (alleged to be the same altoid who originally announced Silk Road's presence) posts a job ad for an "IT pro in the Bitcoin community" to work in a "venture-backed Bitcoin startup company". Interested parties are asked to write to **"rossulbricht at gmail dot com."** Allegedly, this post links 'altoid' to Ross Ulbricht, putting him under the authorities' suspicion.

Silk Road—Trails (2)

- **Feb. 5, 2012: Dread Pirate Roberts**
  On Silk Road forums, user "Silk Road" announces "I need an identity separate from the site and the enterprise of which I am now only a part. I need a name. Drum roll please..... my new name is: Dread Pirate Roberts". This becomes the official forum mouthpiece for Silk Road.
- **Nov. 11, 2011:** Dread Pirate Asks Stackoverflow For Tech Tips
  Someone creates an account on programming advice site StackOverflow.com with the name 'Ross Ulbricht' and email address **rossulbricht@gmail.com**.
  - The curl script posted in the above Stack Overflow question is identical to code obtained from one of the Silk Road servers.

Silk Road—The End

- **July 23, 2013**
  The FBI Gets An Image of The Silk Road Server
- **July 24, 2013—July 31, 2013**
  Homeland Security Confronts Ulbricht
- **Oct. 1, 2013**
  Ulbricht is Arrested
- **Oct. 2, 2013**
  Silk Road Seized By Law Enforcement
  Bitcoin value crashes
  Vendors arrested

Silk Road—Subpoenas

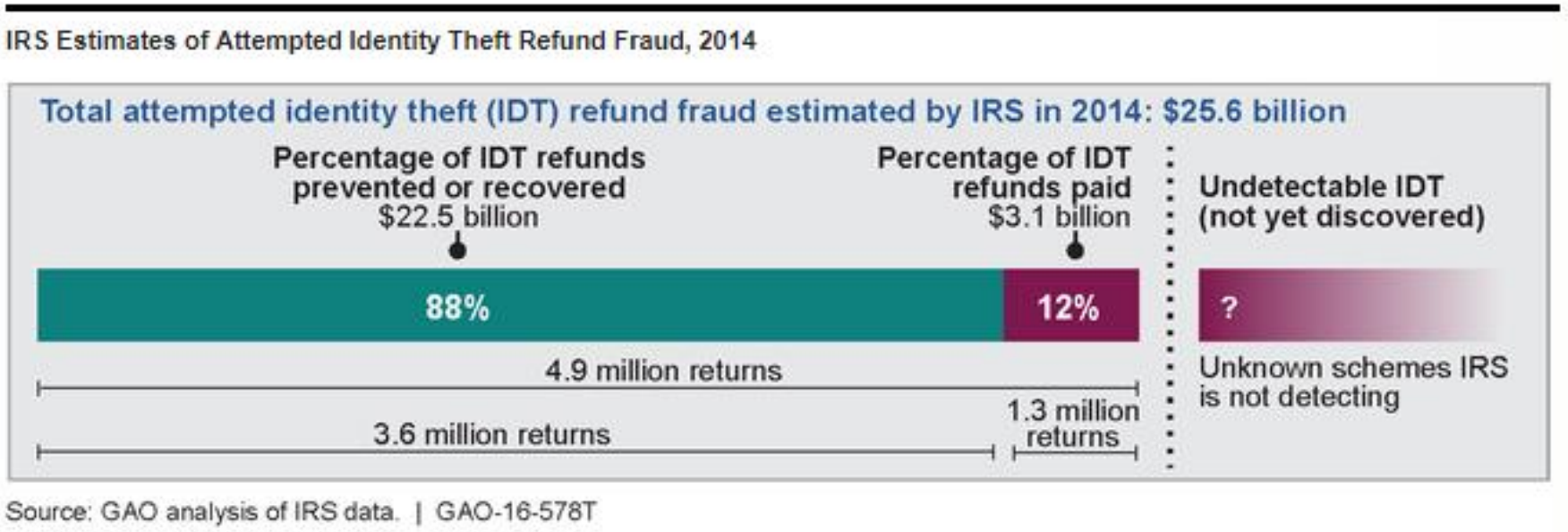
- **A subpoena to Google provided information about the accountholder**
  - details of IP addresses used to log into Mr. Ulbricht's account (San Francisco, specifically an internet cafe on Laguna Street)
  - IP address is a VPN server
- **VPN server's records were obtained by FBI**
  - VPN server's records indicated a user had accessed it from a San Francisco Internet café near the home of a friend Ulbricht had gone to live with
- **The FBI Gets An Image of The Silk Road Server**
  - hosting provider at the request of the FBI via local authorities and the Mutual Legal Assistance Treaty.

Silk Road—Gaps?

- **FBI claimed it was because of a misconfiguration of the site's CAPTCHA, which inadvertently revealed Silk Road's IP address.**
  - Doubts about this claim
  - Someone claim the attack on Tor around the same time is related

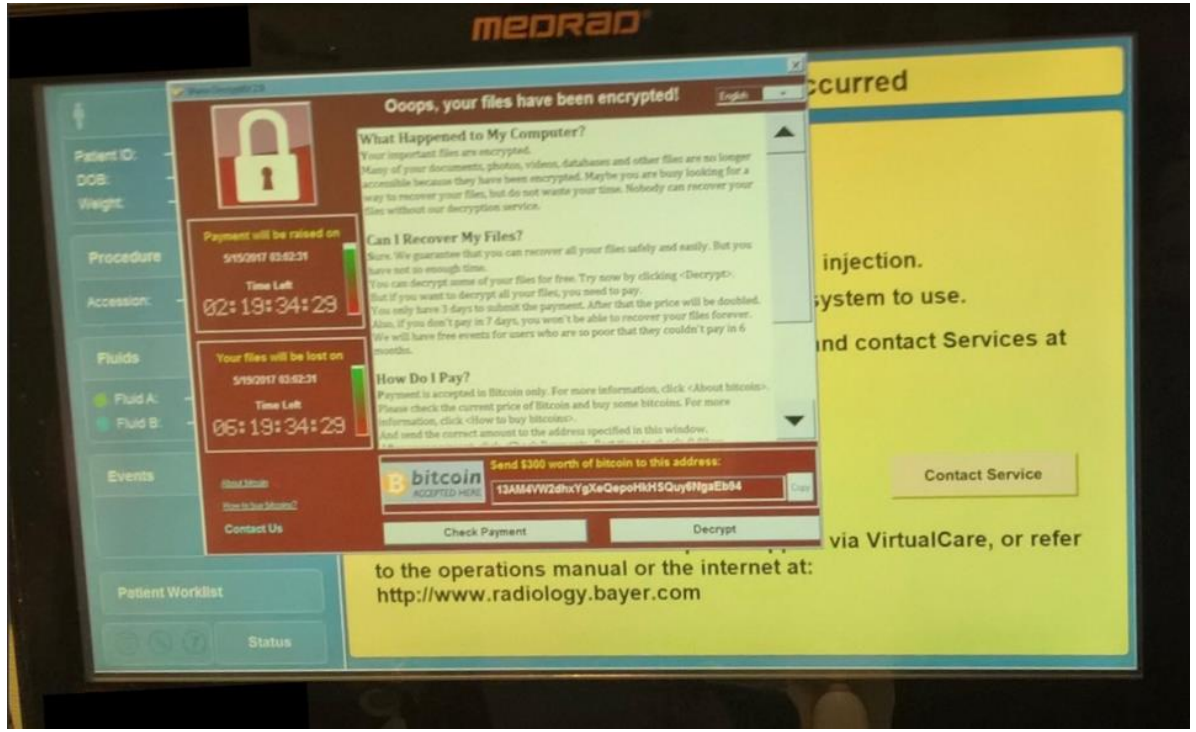
New approaches

- **Race to file tax returns**



Ransomware

- Possible reuse of intelligence agency tools



More Ransomware

- **Colonial Pipeline Cyber Attack – May 7, 2021**
  - Paid $4.4 million ransom
  - Pipeline restarted after 5 days
  - FBI recovered 63.7/75 bitcoins of ransom
- **Meat supplier JBS – June 2021**
  - Paid $11M ransom

Takeaway

- **Online crime is increasing in magnitude**
  - Search-redirection for online pharmacies:
    - top 12 clusters account for 2/3 activity
    - Few, large, traffic brokers
  - Large number of participants perhaps induced by these “big shots”
    - This plays to the advantage of the defender!
    - Disrupt dependencies of the underground market
- **Darknets**
  - Use Tor hidden service
  - Police manage to collect enough information to shut down many
  - Top Tor Darknet Links 2021 to Visit
- **New approaches being created**