What's Clicking What?

Techniques and Innovations of Today's Clickbots

Brad Miller, **Paul Pearce**

Chris Grier, Christian Kreibich and Vern Paxson

UC Berkeley and ICSI

July 8th, 2011

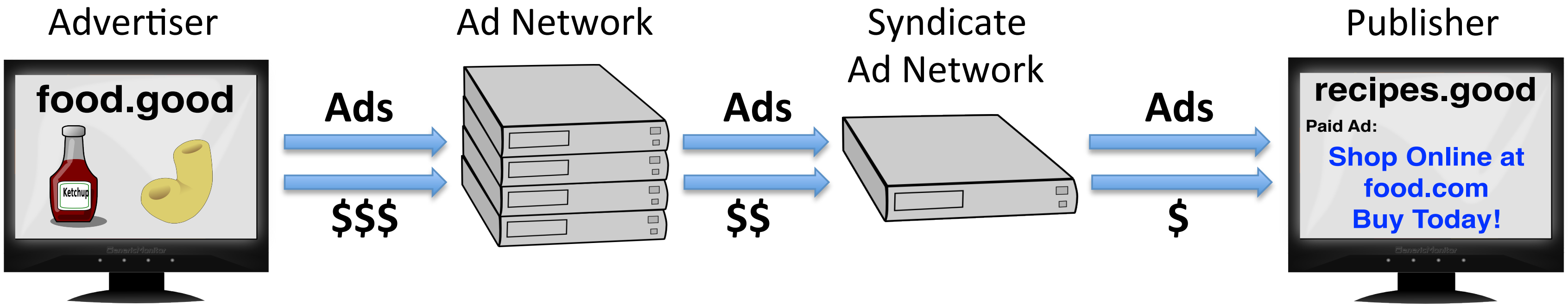
Key Points

- Reverse engineered 2 clickbot networks
  - “Fiesta”, “7cy”
  - Obtained from Pay Per Install services
- Develop click-fraud roles and relationships
  - Job specialization *within* click-fraud
- Analyzed 366,000 click-fraud directives
- Measure human emulating behaviors
  - Timing and location

BACKGROUND

Online Advertising

- Advertiser wants to attract traffic
- Publisher displays ads
- Ad network connects advertisers to publishers
- Syndicate may act as middle-man



Advertiser

food.good

Ad Network

Syndicate Ad Network

Publisher

recipes.good

Paid Ad:

Shop Online at food.com Buy Today!

Ads

$$$

Ads

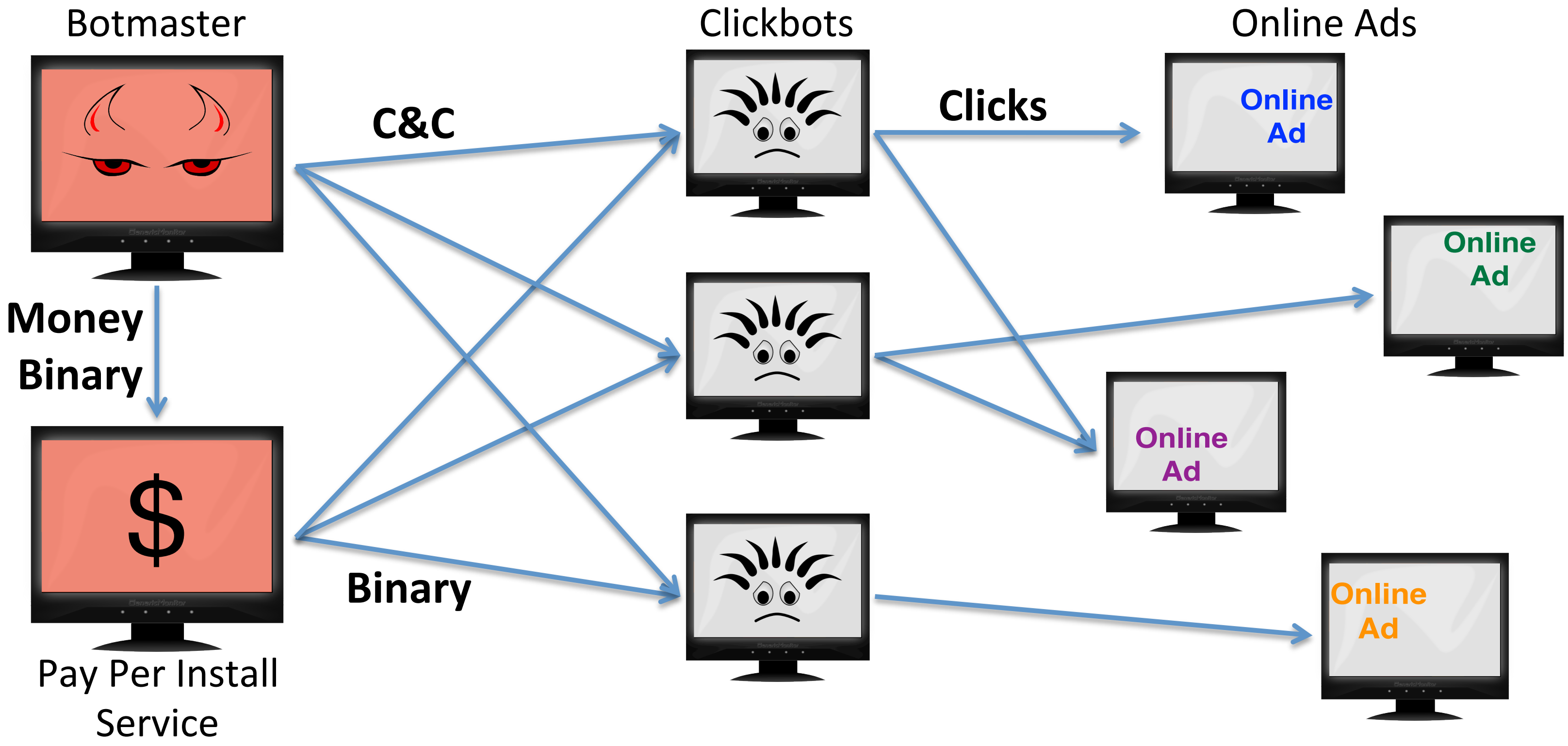
$$

Ads

$

Clickbots = Click-fraud + Botnets

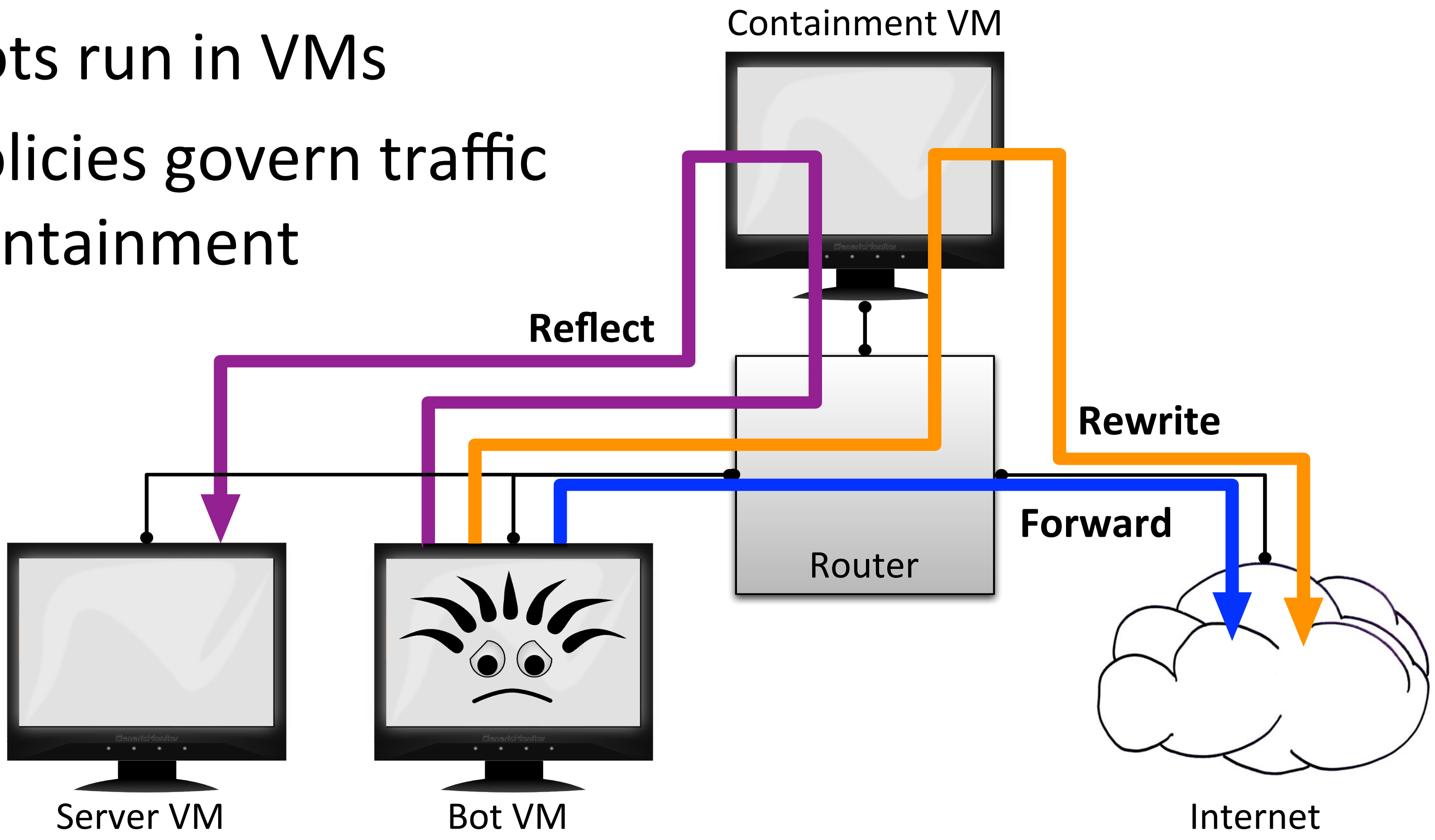
- Command and Control (C&C) protocol



ANALYSIS METHODS

ICSI Honeyfarm

- Bots run in VMs
- Policies govern traffic containment



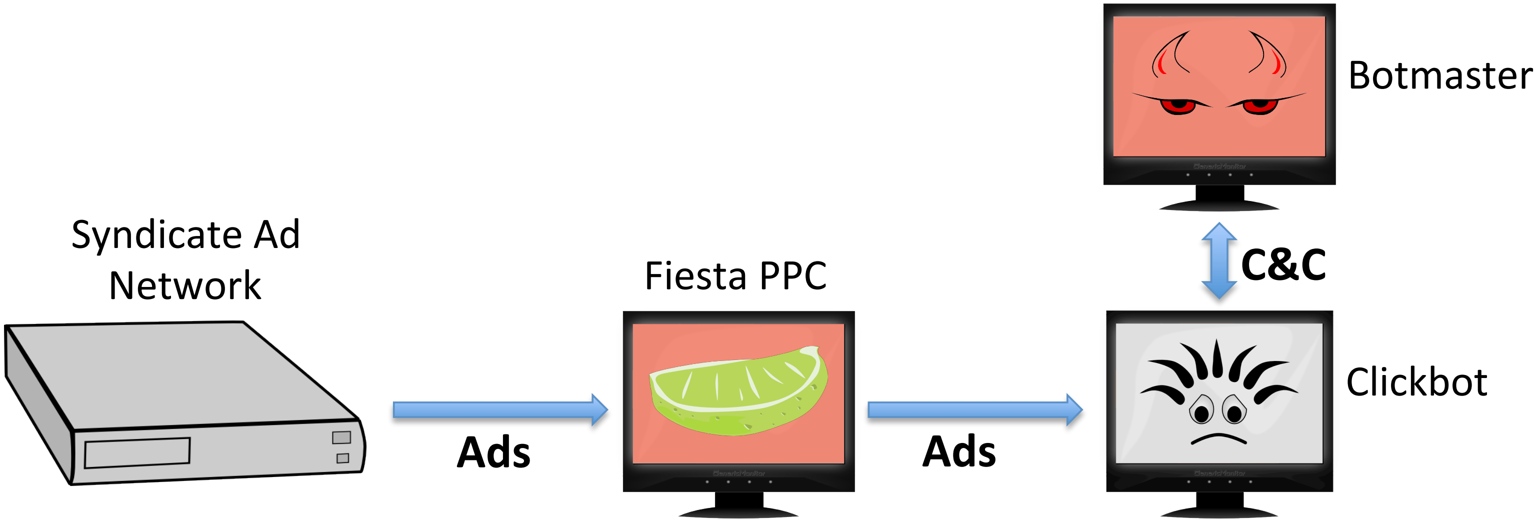
In-Farm Analysis Techniques

- C&C exploration
  - Replay commands
  - Perturb commands
- Webpage emulation
- Real time monitoring of outgoing traffic
- Traffic logging

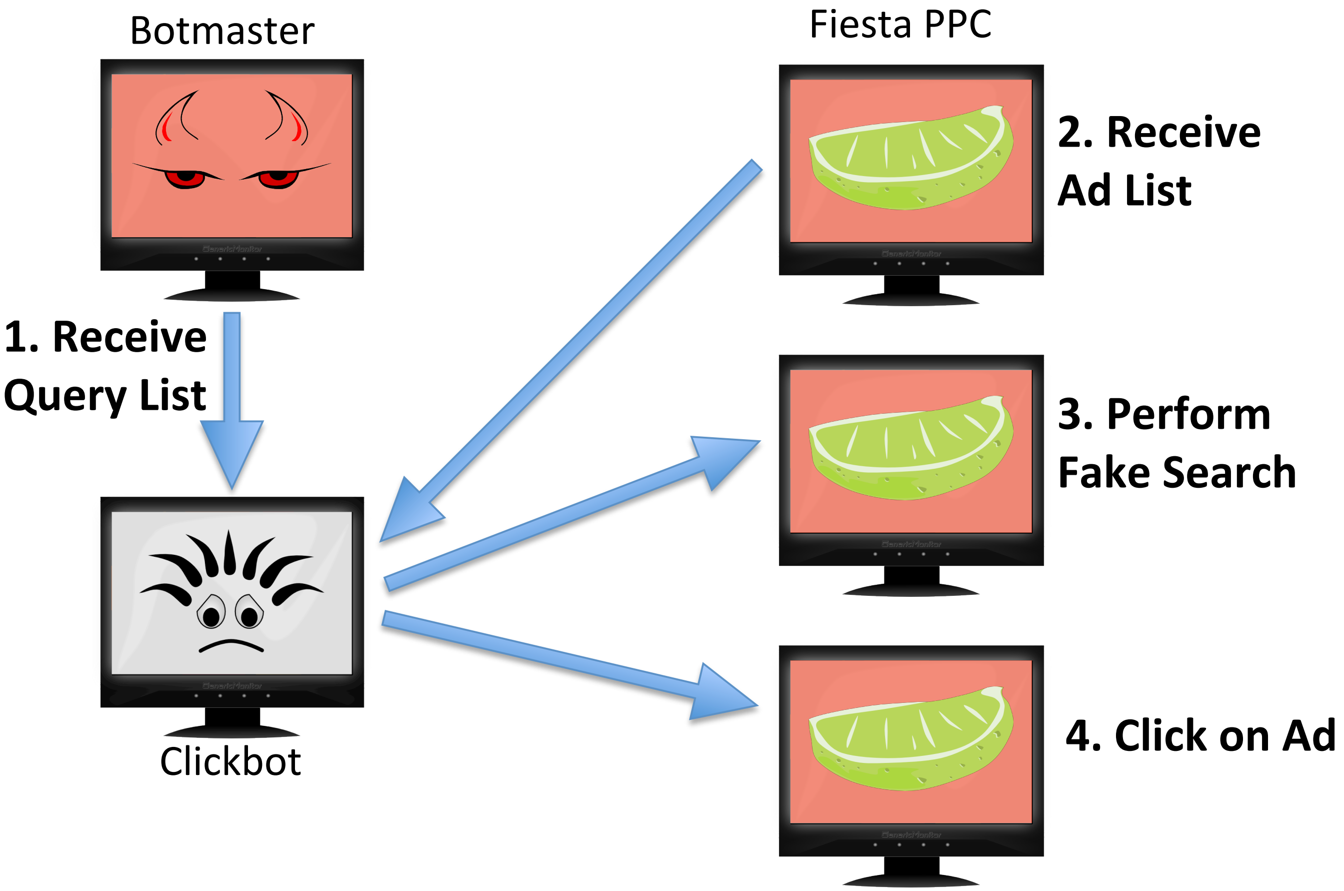
“FIESTA”

Fiesta System Overview

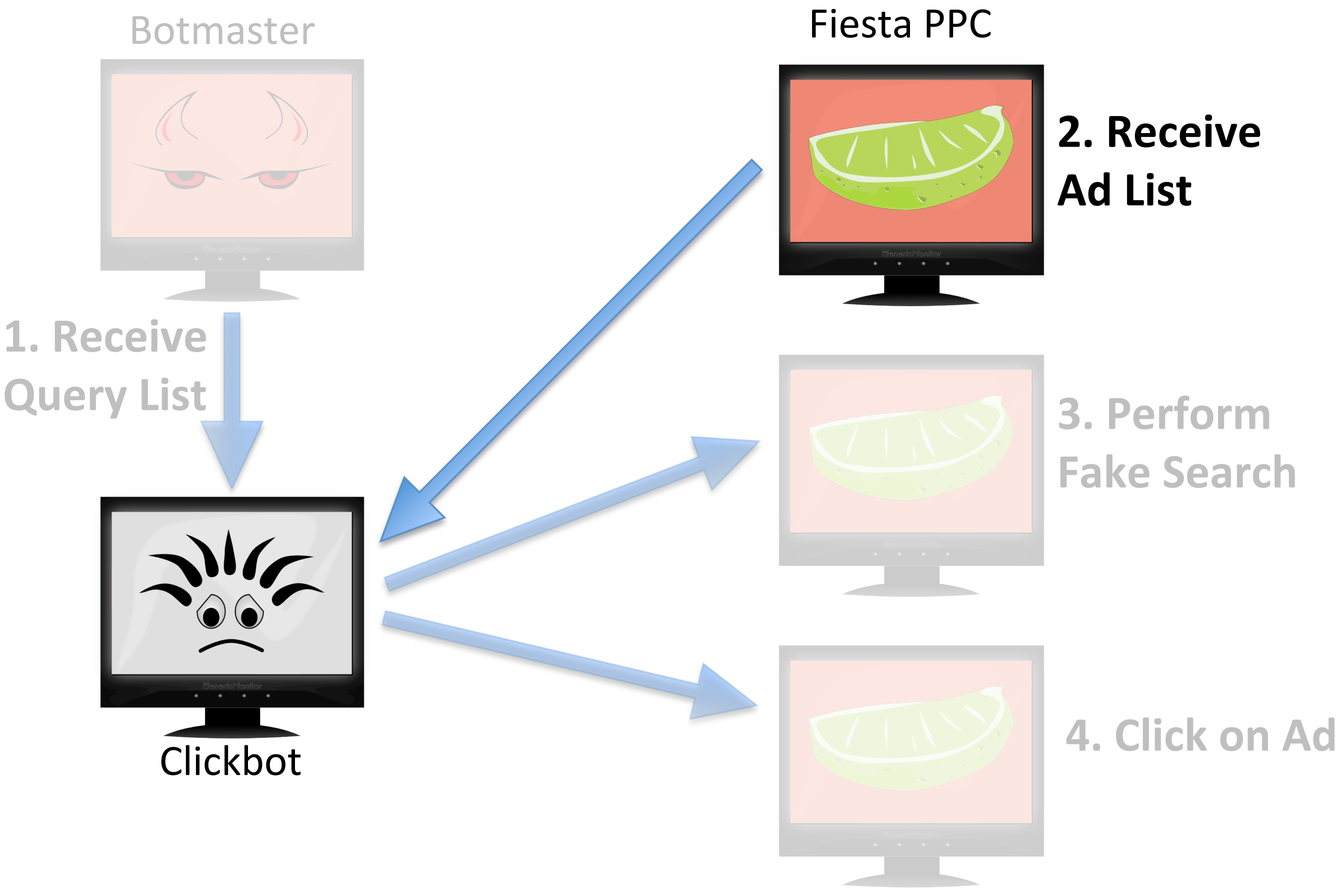
- Bot interacts with middle-man dispensing ads
  - Middle-man is the Fiesta Pay Per Click (PPC) service
  - Ad syndicator supplies ads
  - Fiesta PPC passes ads from syndicator to clickbots
  - 3rd party (botmaster) operates clickbots



Fiesta Fraudcycle



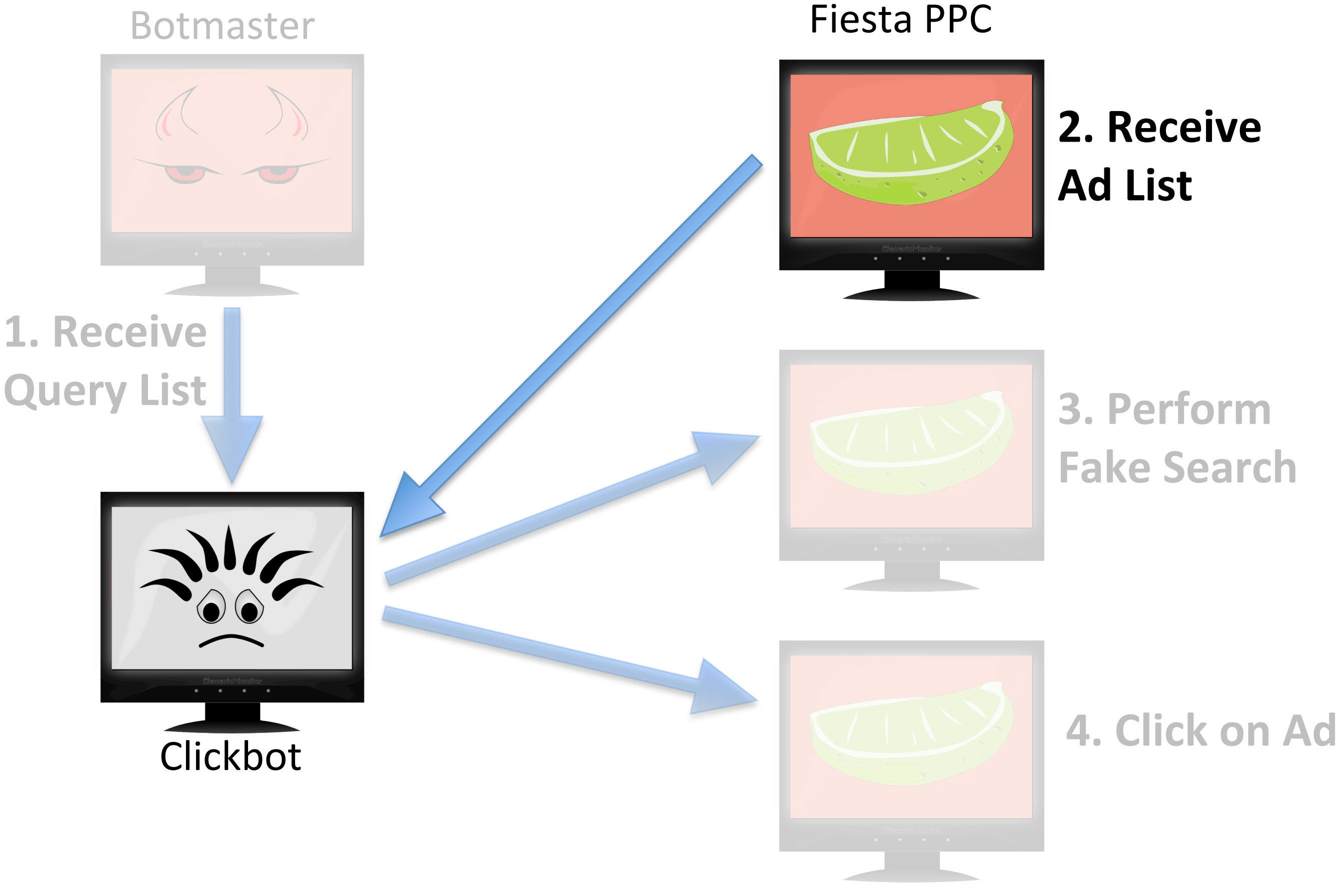
Fiesta Fraudcycle



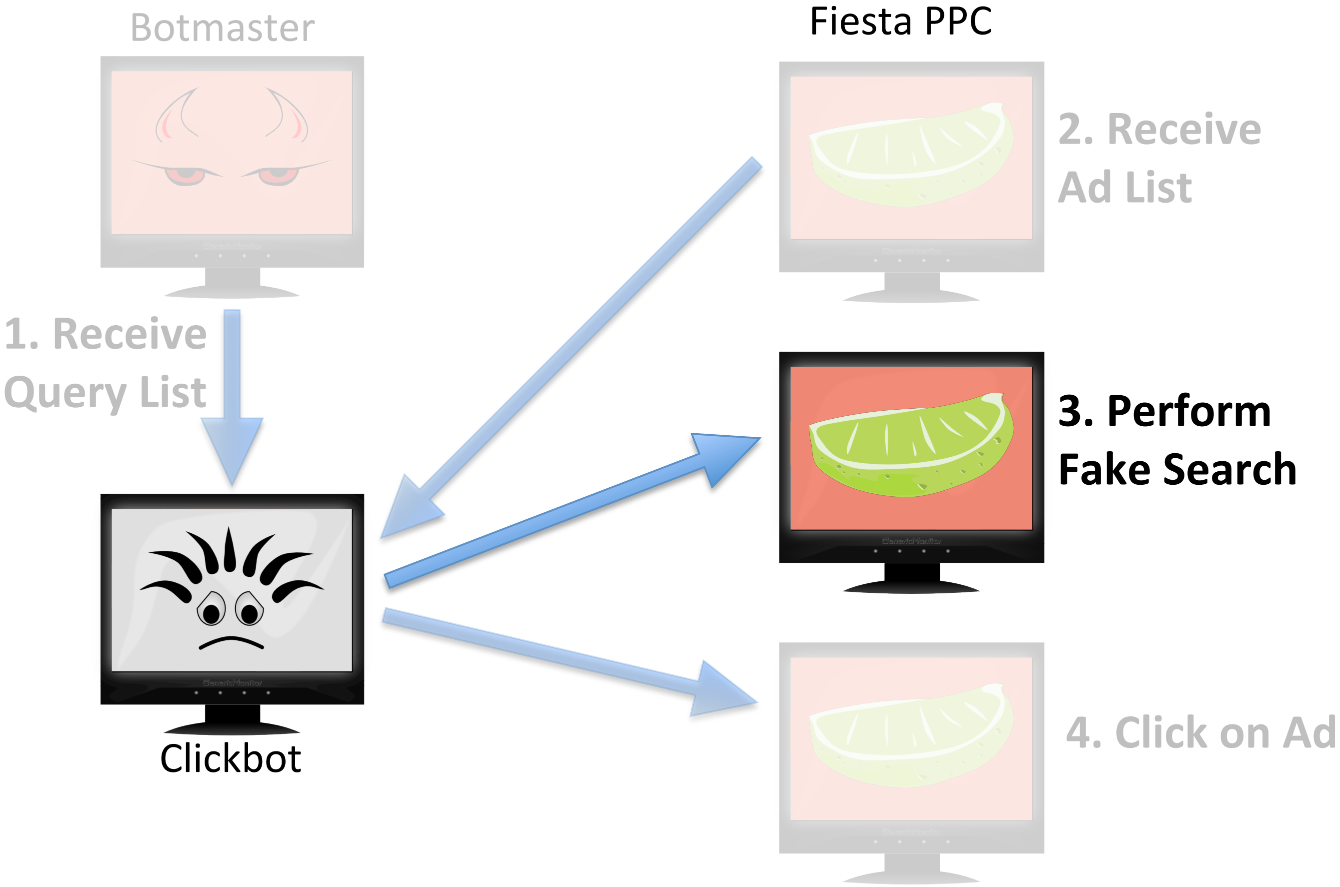
Fiesta Ad Feed (Step 2)

```
<?xml version="1.0" encoding="UTF-8"?>
<records>
 <query>u2 tour</query>
   ...
 <record>
  <title>Looking for u2 tour?</title>
  <description>Find u2 tour here!</description>
  <url>http://u2-tour.com</url>
  <clickurl>http://68.169.64.131/click.php?c=4f820396fcb...</clickurl>
  <bid>0.0004</bid>
  <fi>52</fi>
 </record>
   ...
</records>
```

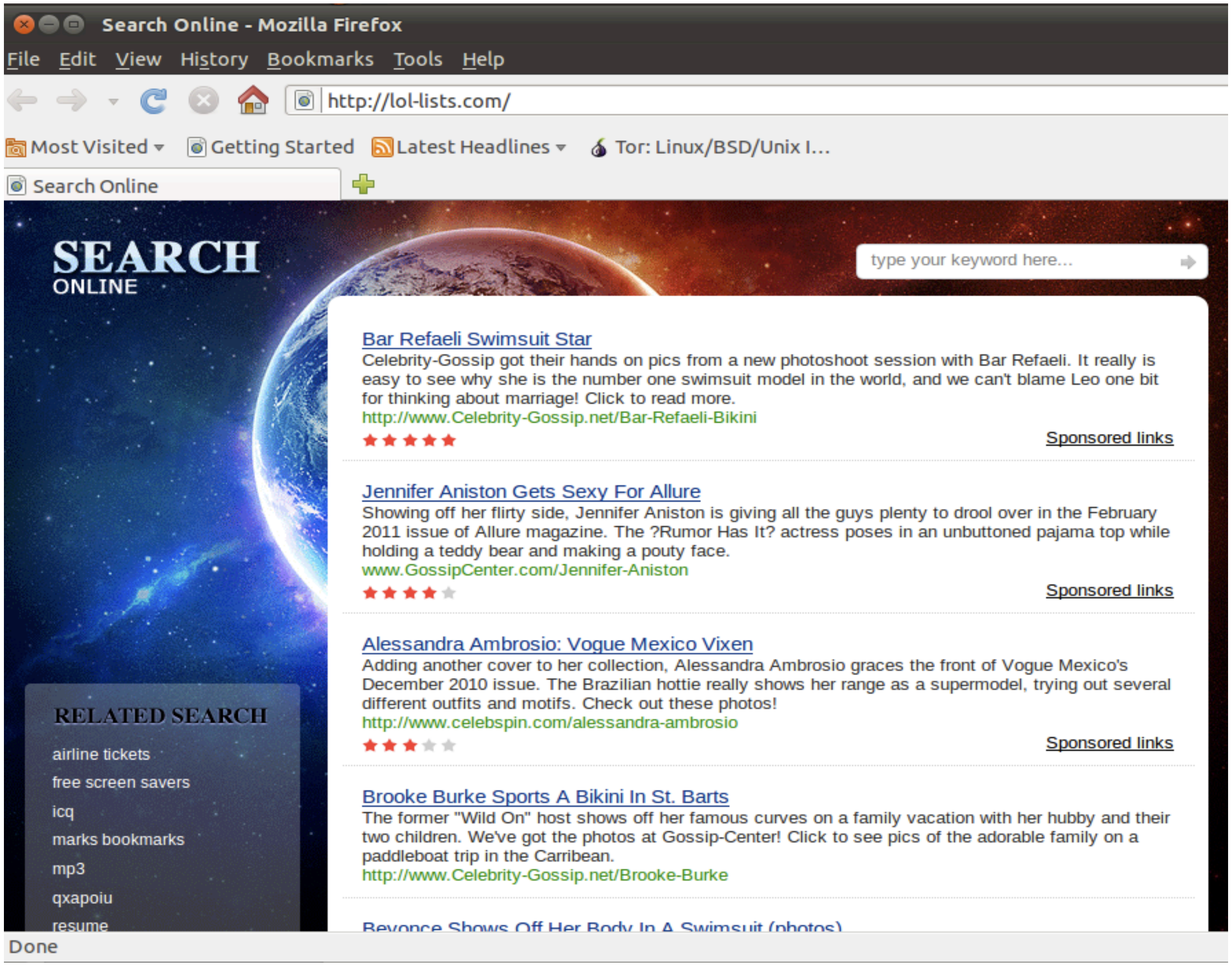
Fiesta Fraudcycle



Fiesta Fraudcycle



Fiesta Fake Search (Step 3)



[Bar Refaeli Swimsuit Star]
Celebrity-Gossip got their hands on pics from a new photoshoot session with Bar Refaeli. It really is easy to see why she is the number one swimsuit model in the world, and we can't blame Leo one bit for thinking about marriage! Click to read more.
http://www.Celebrity-Gossip.net/Bar-Refaeli-Bikini
★★★★★ Sponsored links

[Jennifer Aniston Gets Sexy For Allure]
Showing off her flirty side, Jennifer Aniston is giving all the guys plenty to drool over in the February 2011 issue of Allure magazine. The ?Rumor Has It? actress poses in an unbuttoned pajama top while holding a teddy bear and making a pouty face.
www.GossipCenter.com/Jennifer-Aniston
★★★★☆ Sponsored links

[Alessandra Ambrosio: Vogue Mexico Vixen]
Adding another cover to her collection, Alessandra Ambrosio graces the front of Vogue Mexico's December 2010 issue. The Brazilian hottie really shows her range as a supermodel, trying out several different outfits and motifs. Check out these photos!
http://www.celebspin.com/alessandra-ambrosio
★★★☆☆ Sponsored links

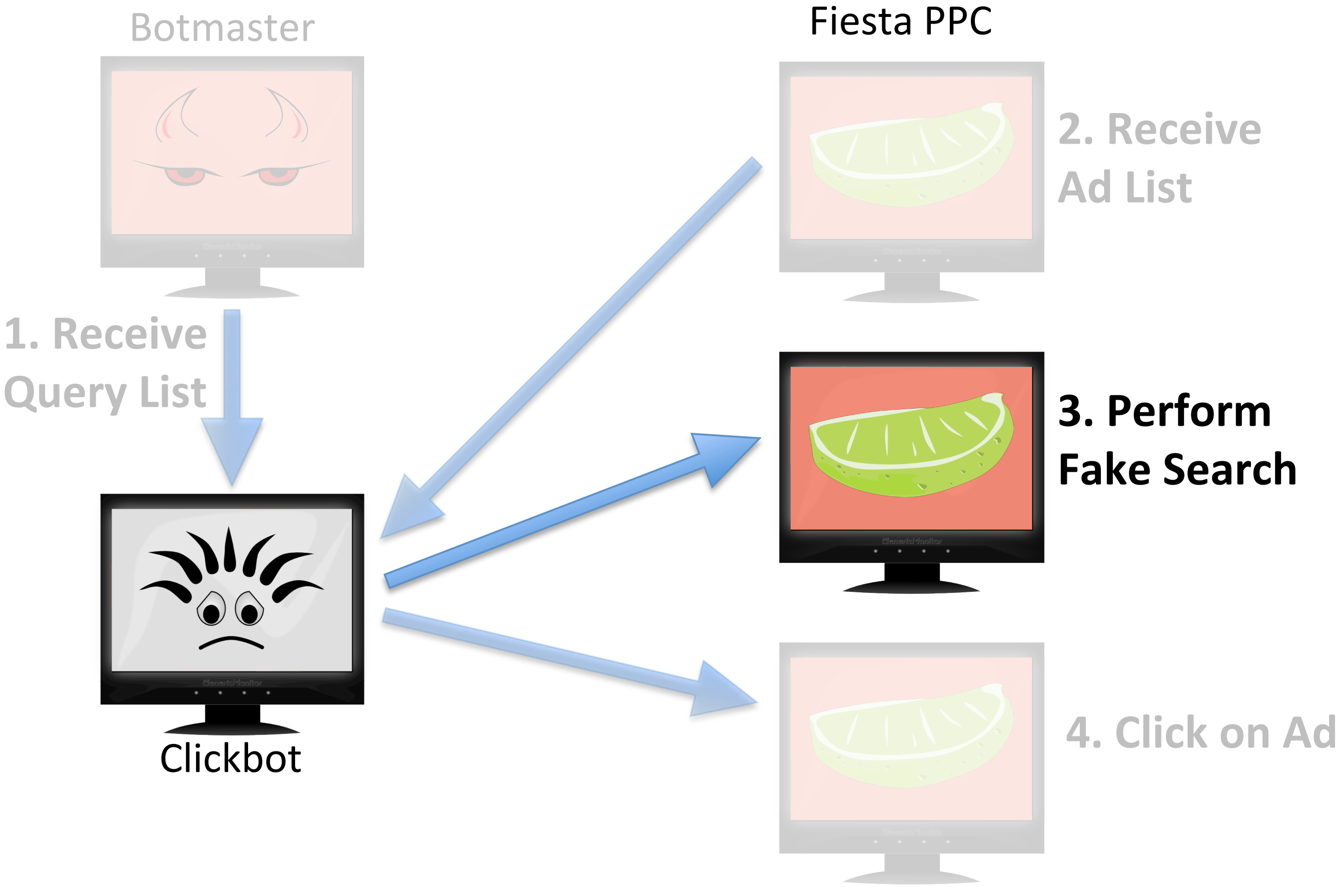
[Brooke Burke Sports A Bikini In St. Barts]
The former "Wild On" host shows off her famous curves on a family vacation with her hubby and their two children. We've got the photos at Gossip-Center! Click to see pics of the adorable family on a paddleboat trip in the Carribean.
http://www.Celebrity-Gossip.net/Brooke-Burke

Beyonce Shows Off Her Body In A Swimsuit (photos)

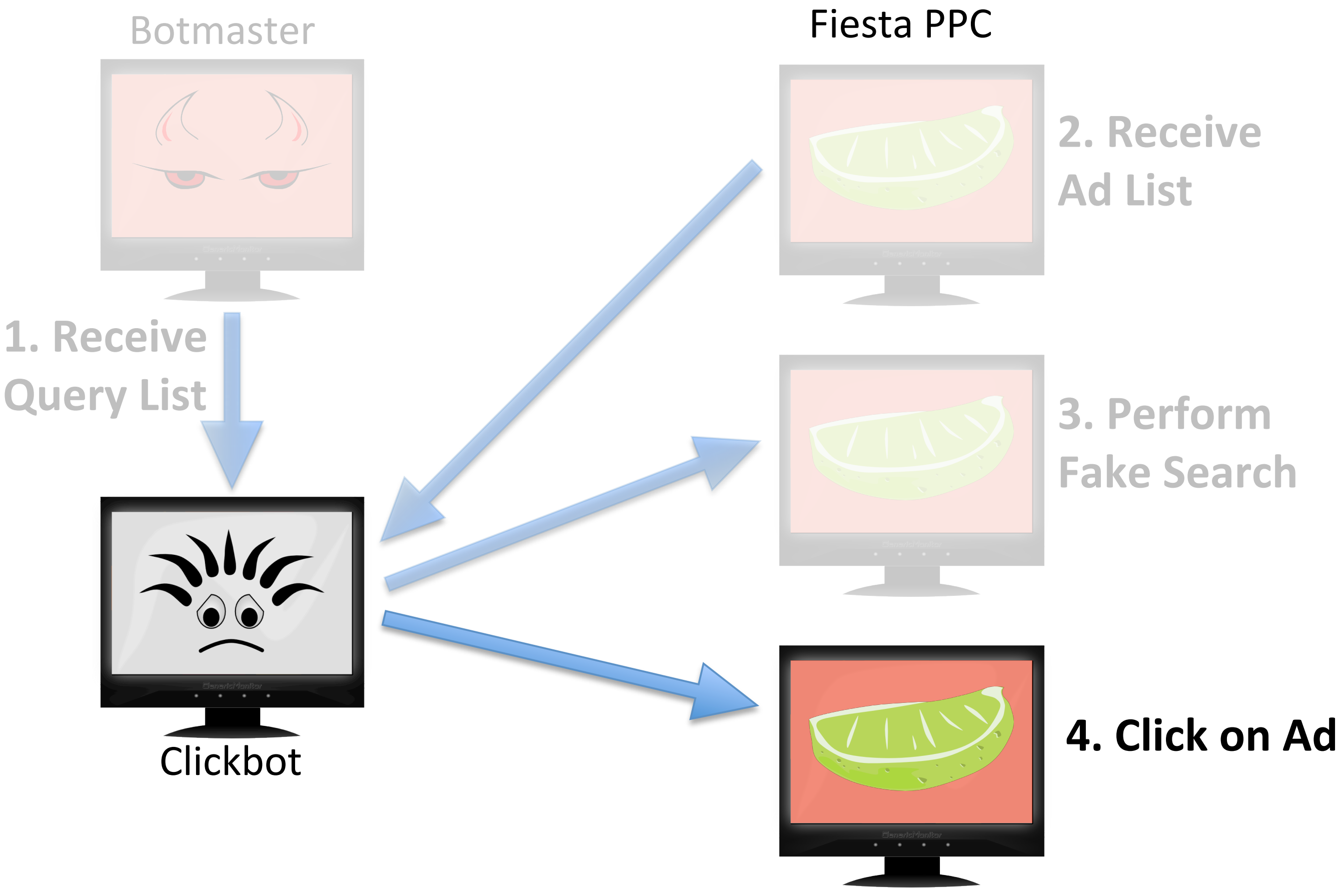
RELATED SEARCH

- airline tickets
- free screen savers
- icq
- marks bookmarks
- mp3
- qxapoiu
- resume

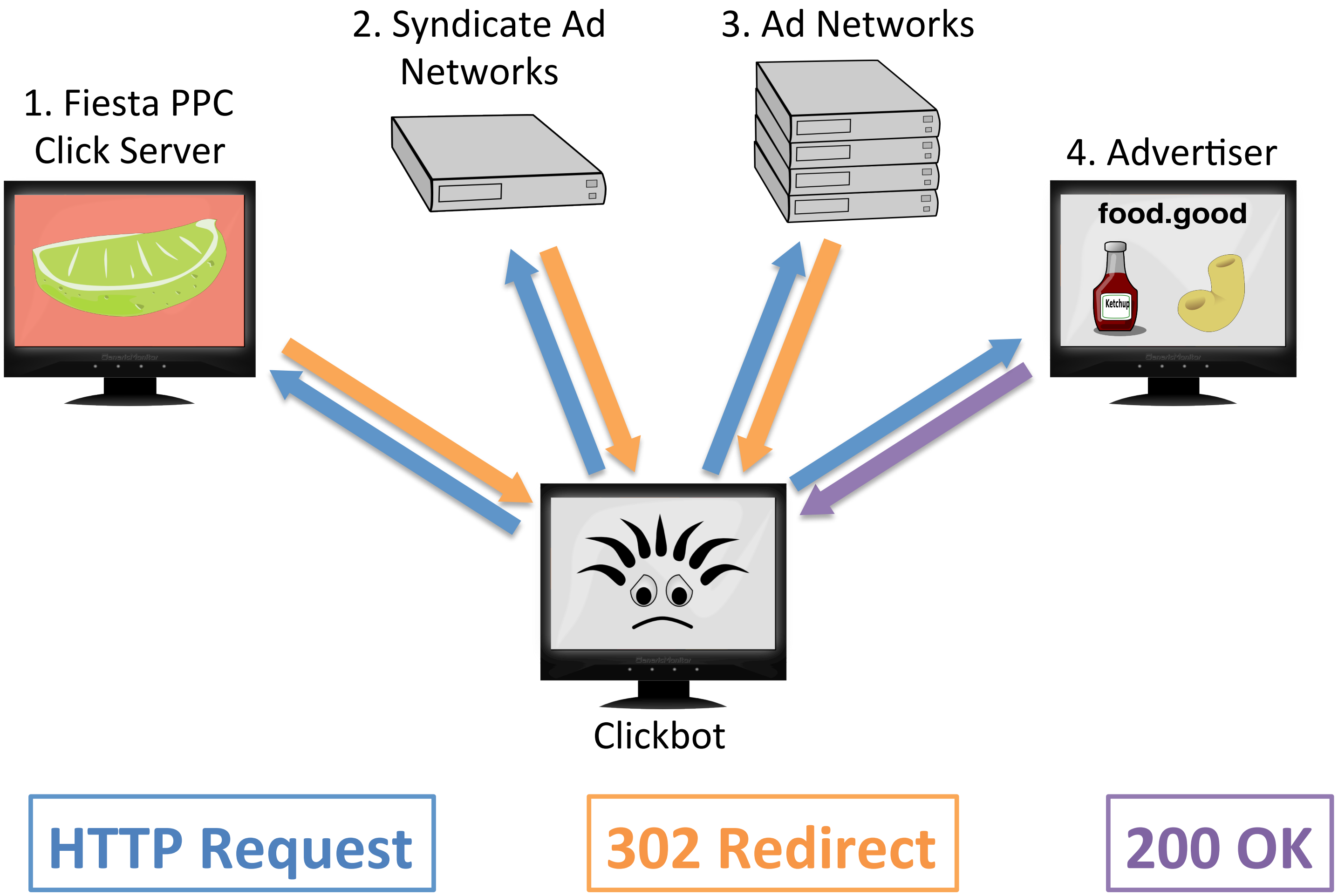
Fiesta Fraudcycle



Fiesta Fraudcycle



Fiesta Ad Click Redirection Chains



1. Fiesta PPC Click Server

2. Syndicate Ad Networks

3. Ad Networks

4. Advertiser

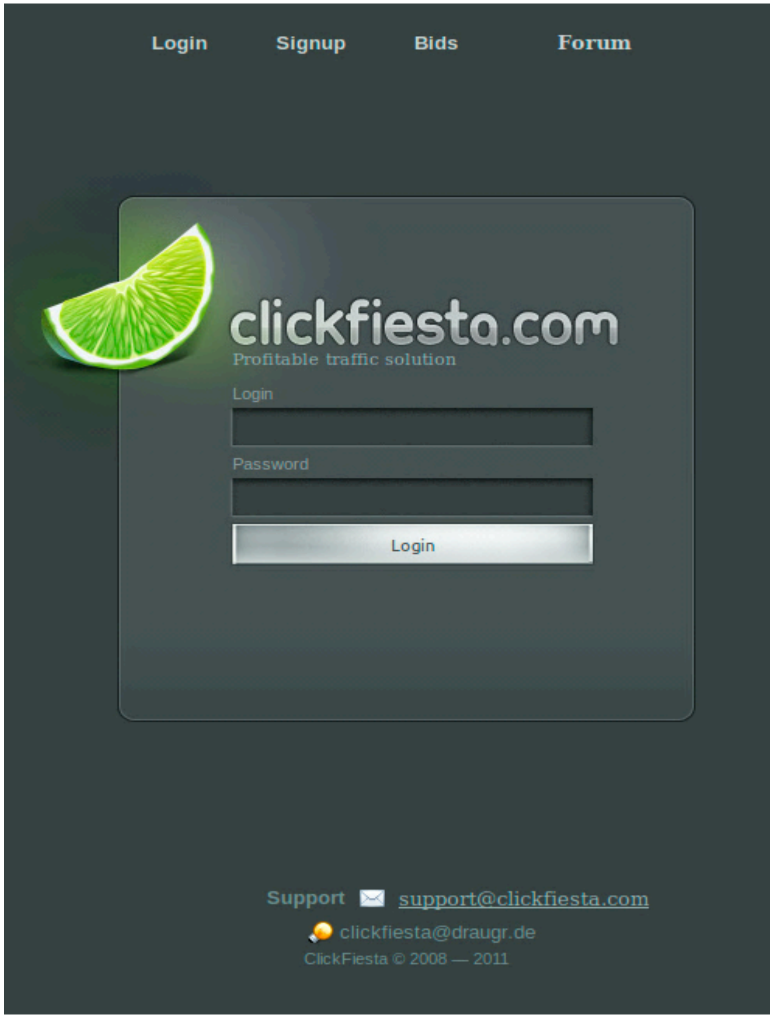
Clickbot

HTTP Request

302 Redirect

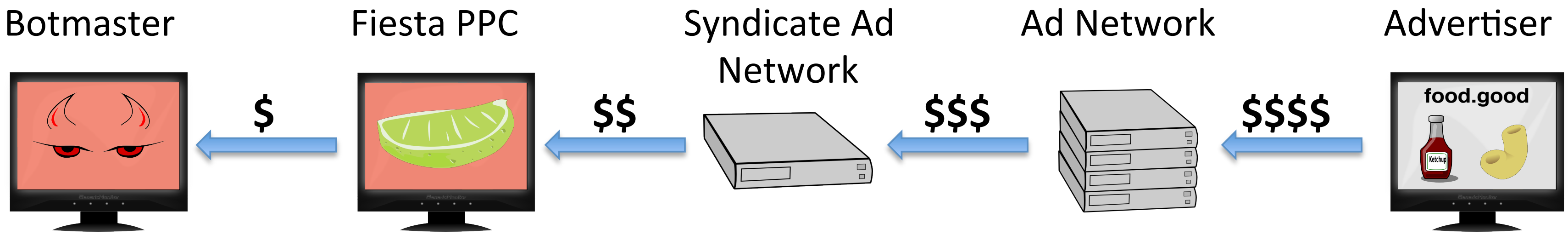
200 OK

Fiesta Storefront


Login
Signup
Bids
Forum
clickfiesta.com
Profitable traffic solution
Login
Password
Login
Support ✉ support@clickfiesta.com
clickfiesta@draugr.de
ClickFiesta © 2008 — 2011

Fiesta Business Relationships

- Fiesta PPC acts as a middle-man
- Job specialization
  - Fiesta PPC focuses on ad networks
  - Bot masters focus on generating traffic
    - Independent study showed the Koobface botnet also generated traffic for Fiesta



Botmaster

$

Fiesta PPC

$$

Syndicate Ad Network

$$$

Ad Network

$$$$

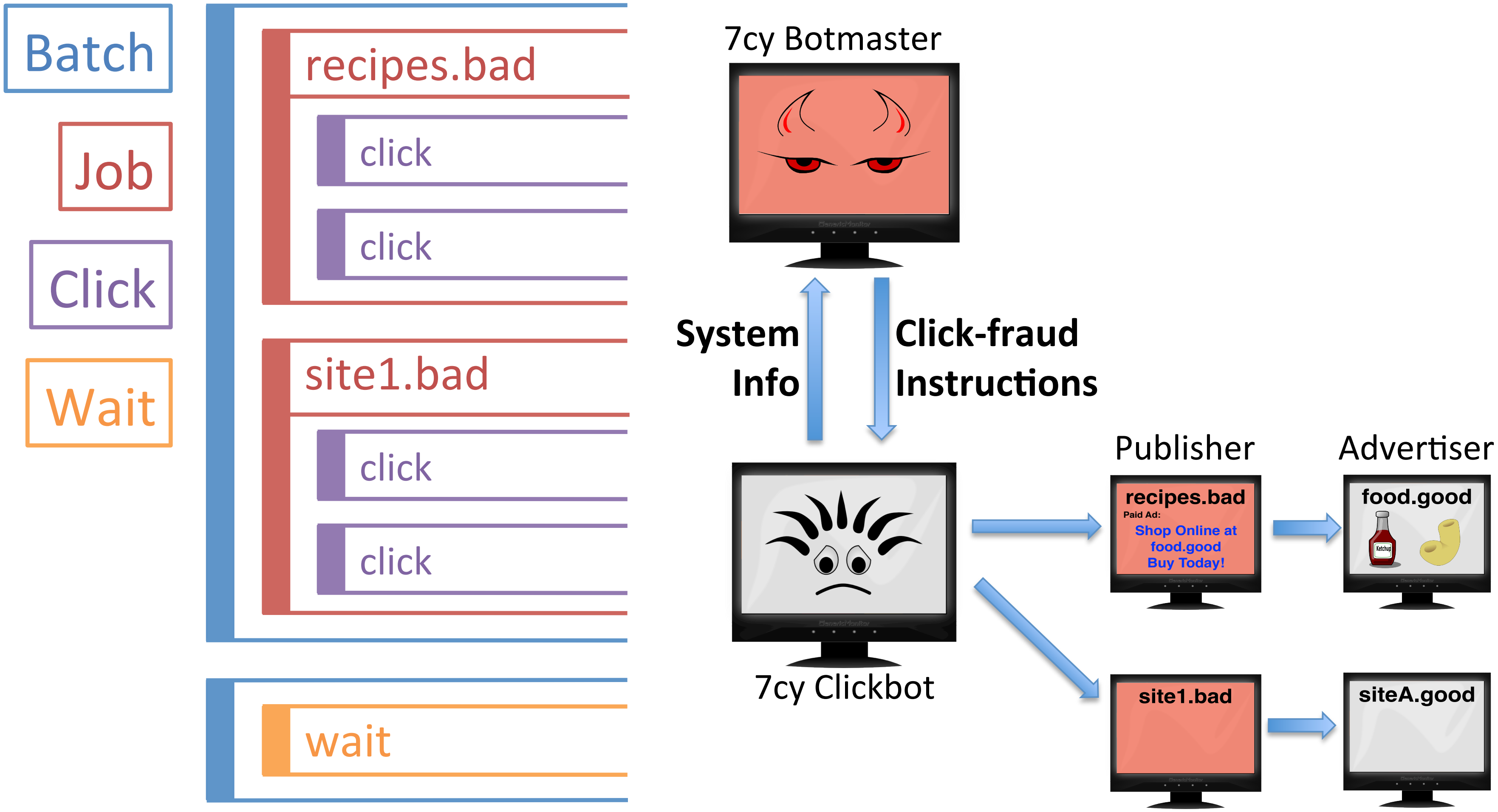
Advertiser

“7CY”

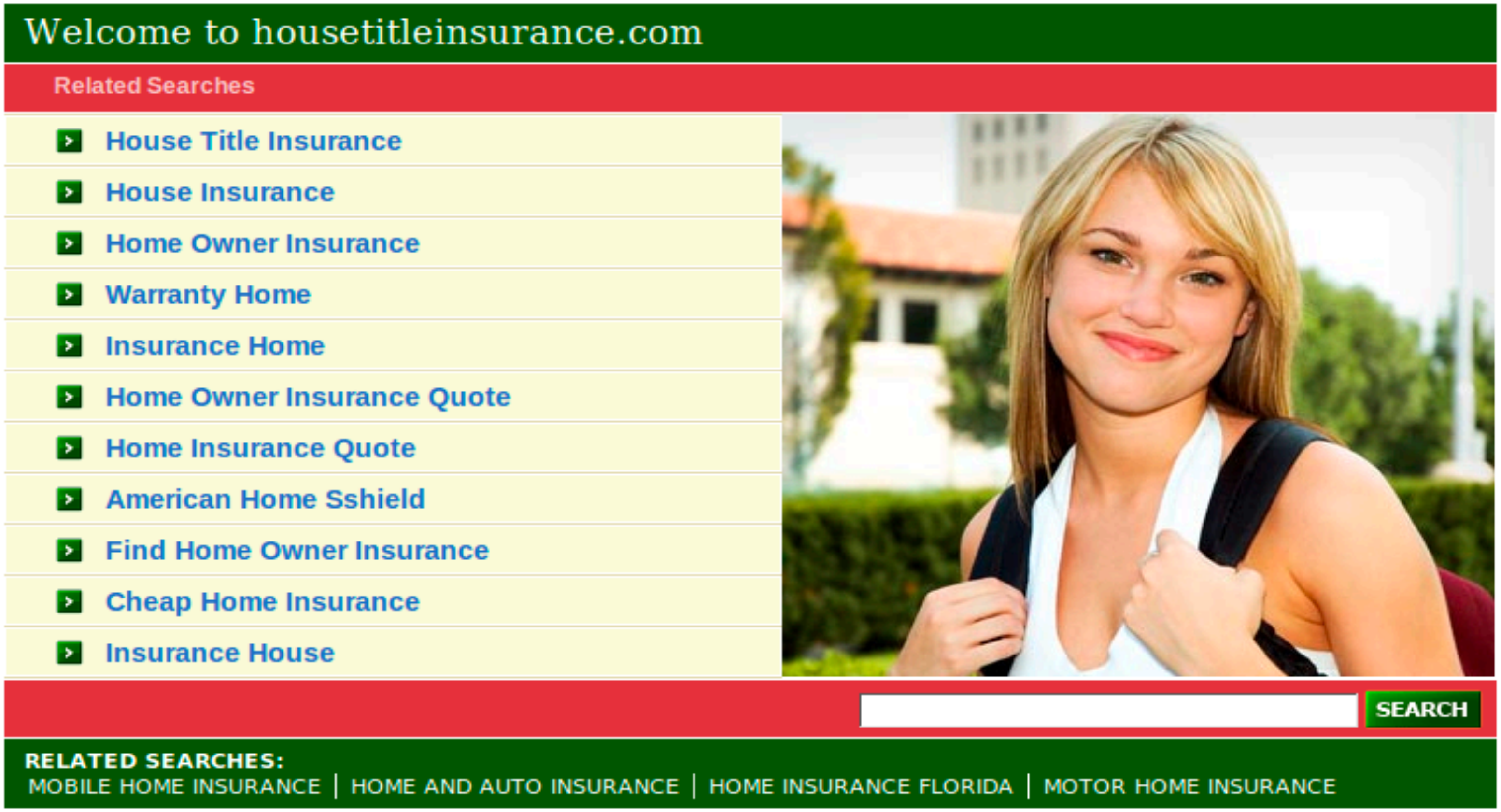
7cy Overview

- Interacts directly with publishers
- Emulates human behavior
  - Timing
    - Delay between clicks
    - Daily traffic pattern
  - Bot location
    - Domains visited
    - Traffic patterns

7cy Fraudcycle



7cy Sample Publisher Site



Welcome to housetitleinsurance.com

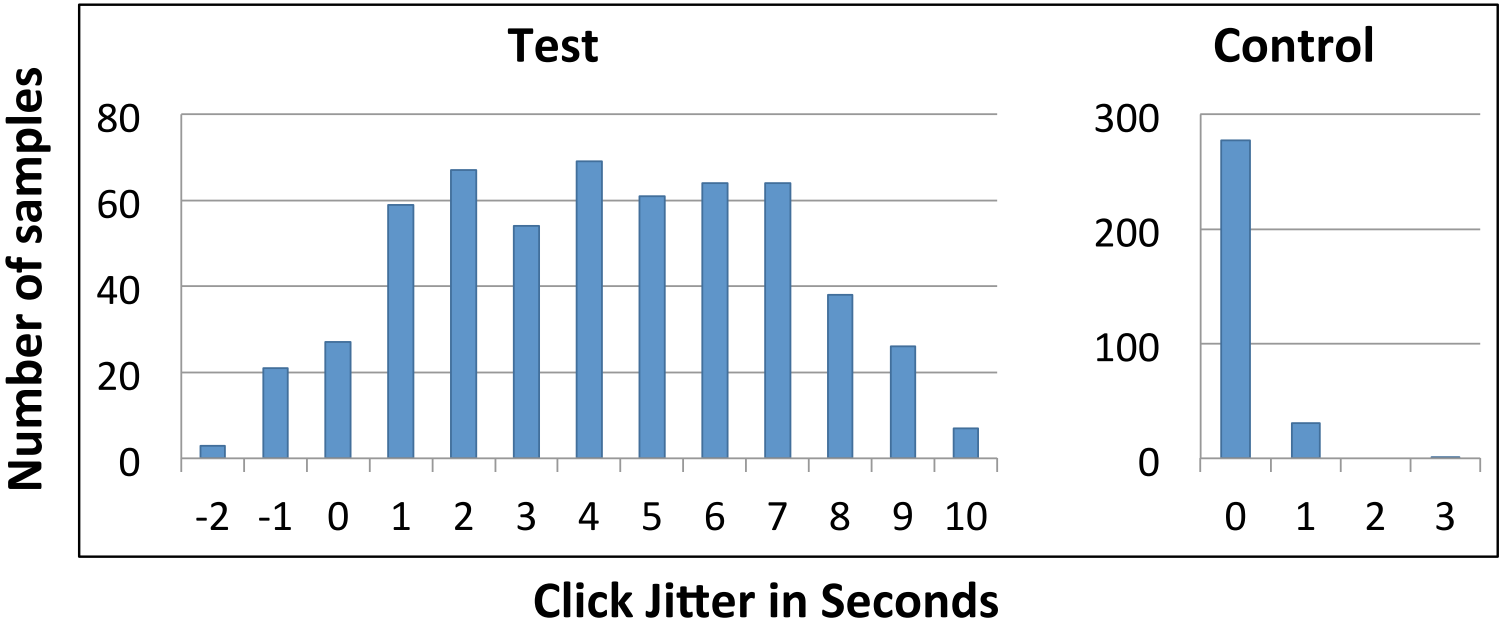
Related Searches

- House Title Insurance
- House Insurance
- Home Owner Insurance
- Warranty Home
- Insurance Home
- Home Owner Insurance Quote
- Home Insurance Quote
- American Home Sshield
- Find Home Owner Insurance
- Cheap Home Insurance
- Insurance House

RELATED SEARCHES:
MOBILE HOME INSURANCE | HOME AND AUTO INSURANCE | HOME INSURANCE FLORIDA | MOTOR HOME INSURANCE

7cy Timing Jitter

- Bot introduced randomness into timed delays
- Comparison between bot and control script

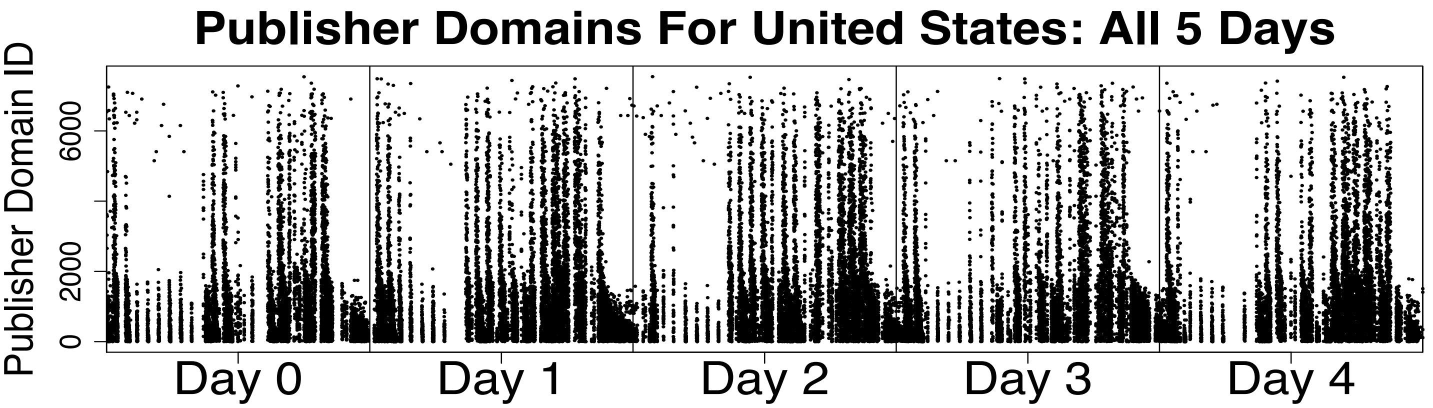


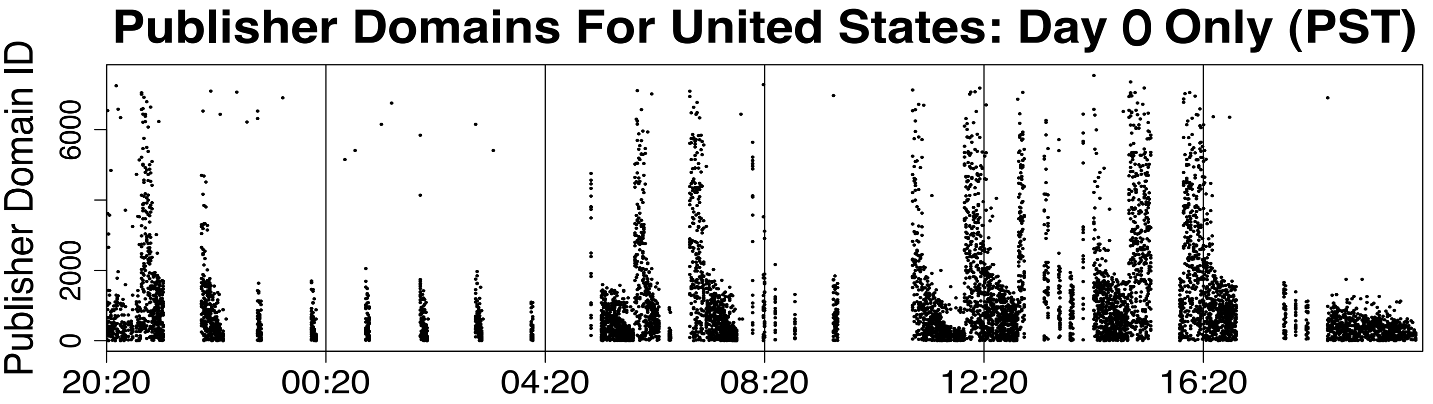
7cy Milker

- Milker emulates actual bot
  - Speaks Command and Control (C&C) protocol
- Tor allows C&C to be gathered around globe
  - 5 days of data
  - Over 366,000 click-fraud directives collected

North America	**Europe**	**East Asia**
Canada	France	Hong Kong
United States	Russia	Japan
	Spain	Singapore
		South Korea

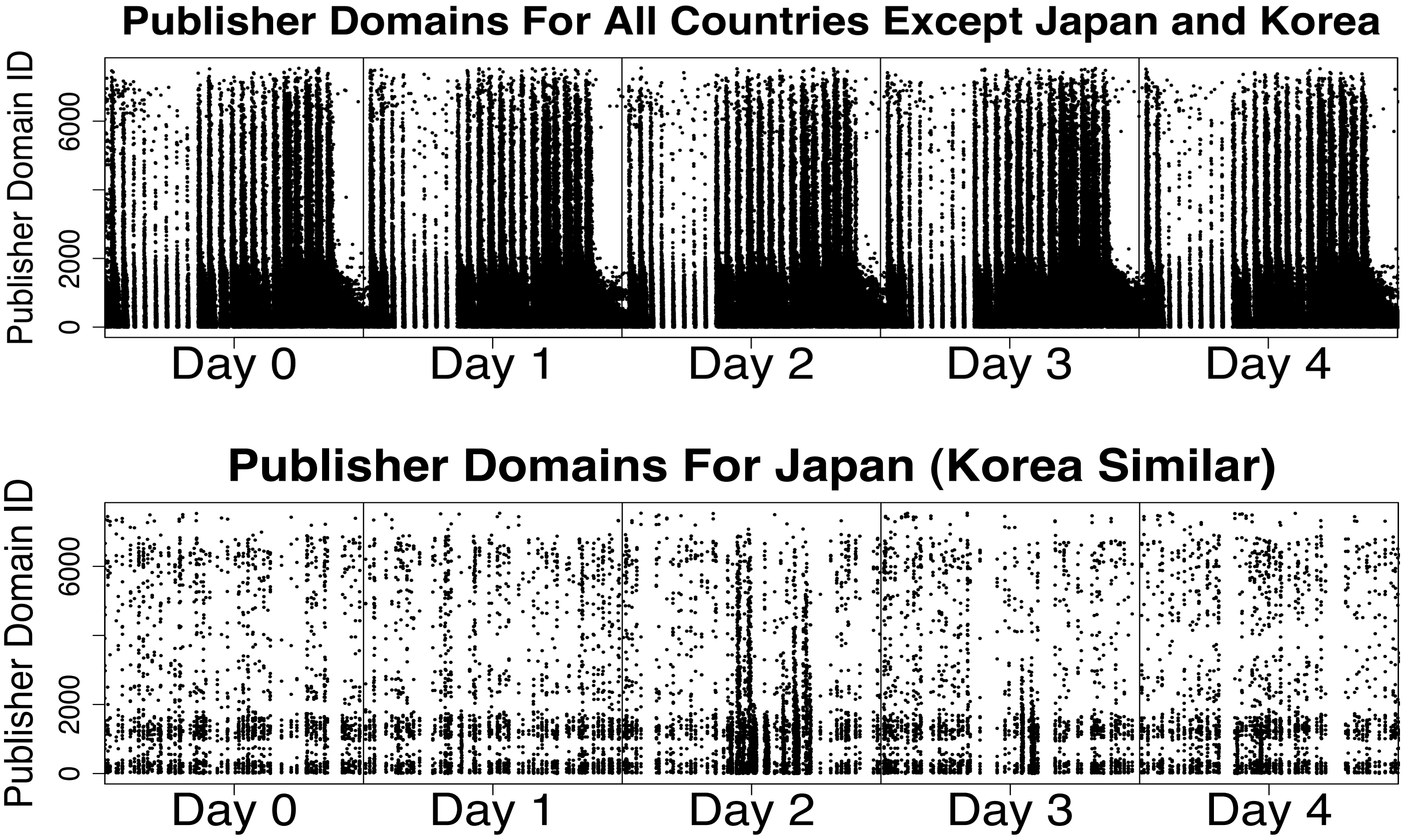
7cy Daily Timing Behavior


Publisher Domains For United States: All 5 Days


Publisher Domains For United States: Day 0 Only (PST)

Traffic volumes vary with time of day and spike hourly

7cy Geographic Timing Behavior



US daily pattern consistent except for Japan and Korea

CONCLUSION

Key Findings

- Fiesta PPC business model
  - Job specialization with click-fraud
- 7cy human emulating behaviors
  - Jitter delay between clicks
  - Location specific behavior
  - Daily timing patterns

Open Questions

- Motivation for location specific behavior?
  - European countries follow American schedule
  - Japanese and Korean domains appear western
- What does 7cy publisher domain traffic look like?
  - Currently under way

QUESTIONS?