

# Parking Sensors: Analyzing and Detecting Parked Domains

Thomas Vissers, Wouter Joosen, Nick Nikiforakis



Stony Brook  
University

# Archetypical Parked Page

Hideemyass.com

Zoekadvertenties

Gesponsorde vermeldingen

Gerelateerde links

- Credit card
- Learn english
- Digital camera webcam
- Pc computers
- Anonymous surfing
- Digital spy camera
- Geld verdienen
- Surf anonymously
- Free email
- Woonruimte

## ▶ [XS USENET & VPN](#)

www.xsusenet.com

SSL Secured Usenet & VPN Up to 120Mbit, as low as 3.19EUR/mo

## ▶ [ALTERNATIVE CRYSTAL SERVE](#)

christiansteven.com/Crystal-Reports

Data driven, event-based, and time based. Server & browser. Free Trial

## ▶ [REALIZING YOUR SPA DREAMS](#)

www.bienfait.be

Le leader mondial des spas, de la qualité pour tous les budgets

## ▶ [WEBMARSHAL.NL](#)

www.webmarshal.nl

Website Content Filtering Web Security, URL filtering en meer

## ▶ [FIND IP ADDRES](#)

www.orangeclimatecontrol.com/

Bespaar op Elektrische aansluiting Verspil geen meter materiaal meer

Gerelateerde links: Digital camera webcam Pc computers Anonymous surfing Digital spy camera Geld verdienen Surf anonymously Free email Woonruimte

# Ecosystem and involved parties

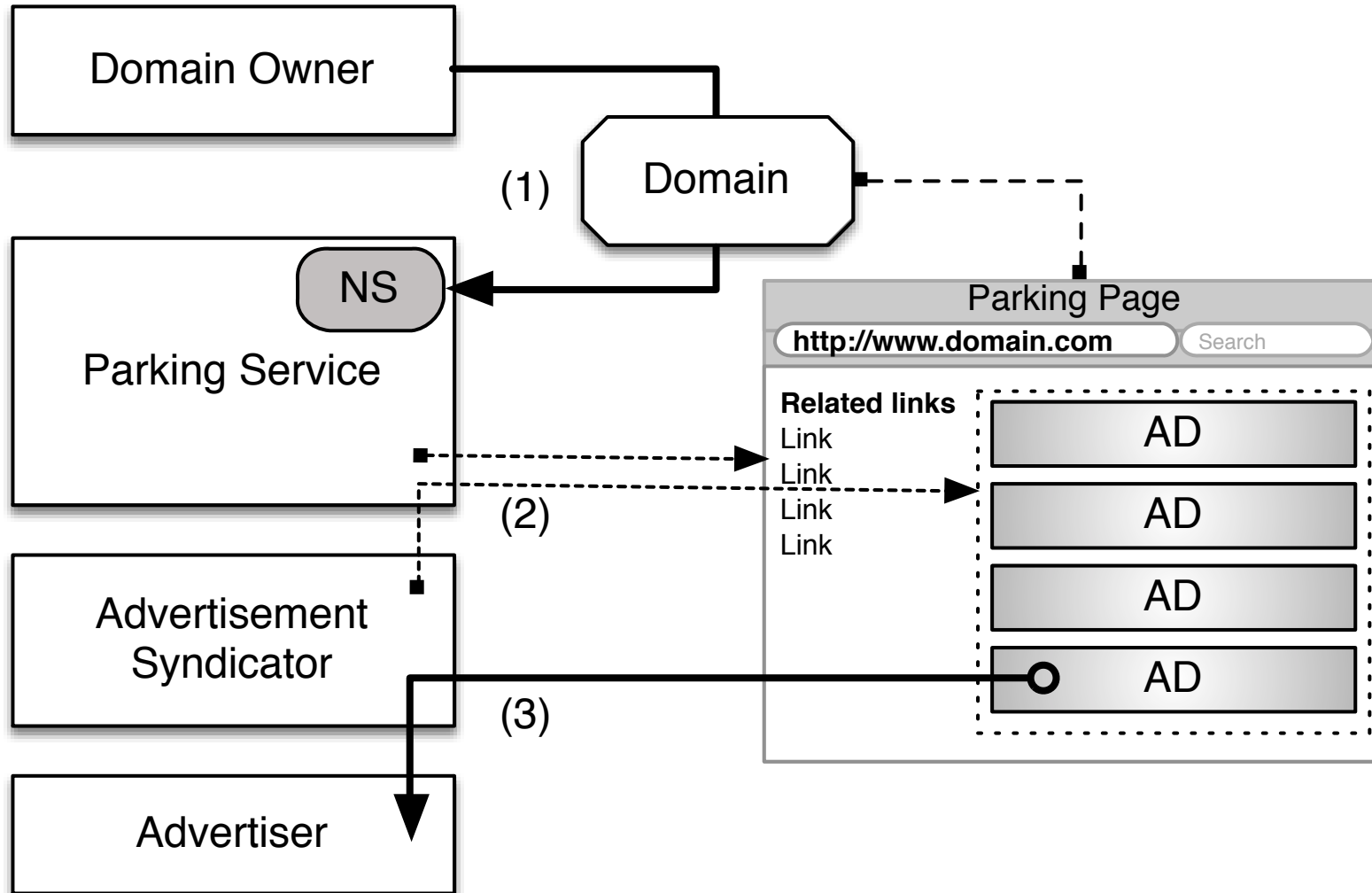
Domain Owner

Parking Service

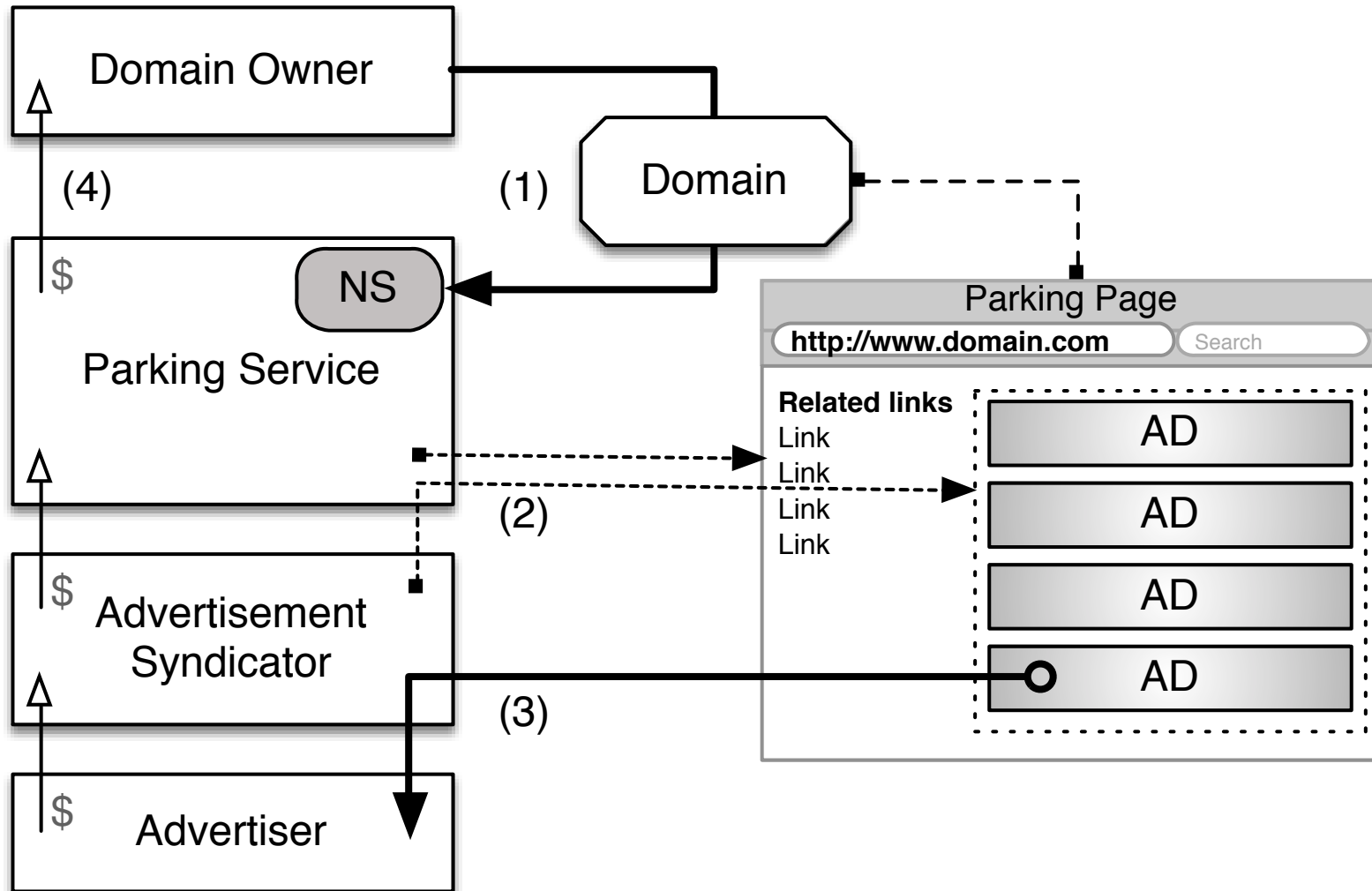
Advertisement  
Syndicator

Advertiser

# Ecosystem and involved parties



# Ecosystem and involved parties



# Research Questions

- What does the ecosystem look like?
  - Involved parties
  - Parking Services
  - Domain Owners
  - Ad Syndicators
  - Bypassing Ad-blockers
- Are they monetizing on abusive domains?
  - Typosquatting abuse
  - Trademark abuse
- Pay-per-Redirection analysis
  - Malicious redirections: malware, scam, adult
- Can we detect parked pages using a classifier?

# Research Questions

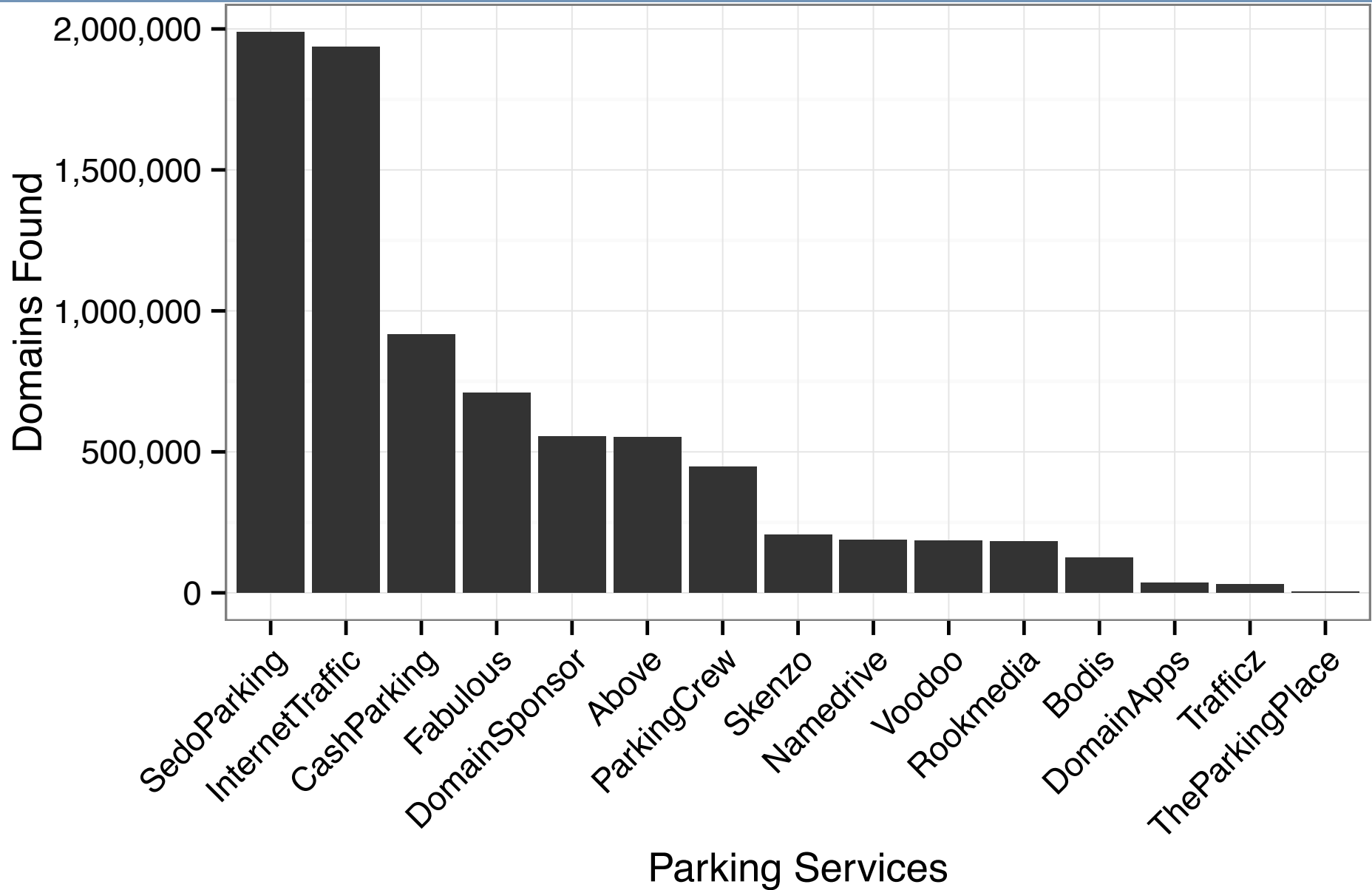
- What does the ecosystem look like?
  - Involved parties
  - Parking Services
  - Domain Owners
  - Ad Syndicators
  - Bypassing Ad-blockers
- Are they monetizing on abusive domains?
  - Typosquatting abuse
  - Trademark abuse
- Pay-per-Redirection analysis
  - Malicious redirections: malware, scam, adult
- Can we detect parked pages using a classifier?

# Research Data

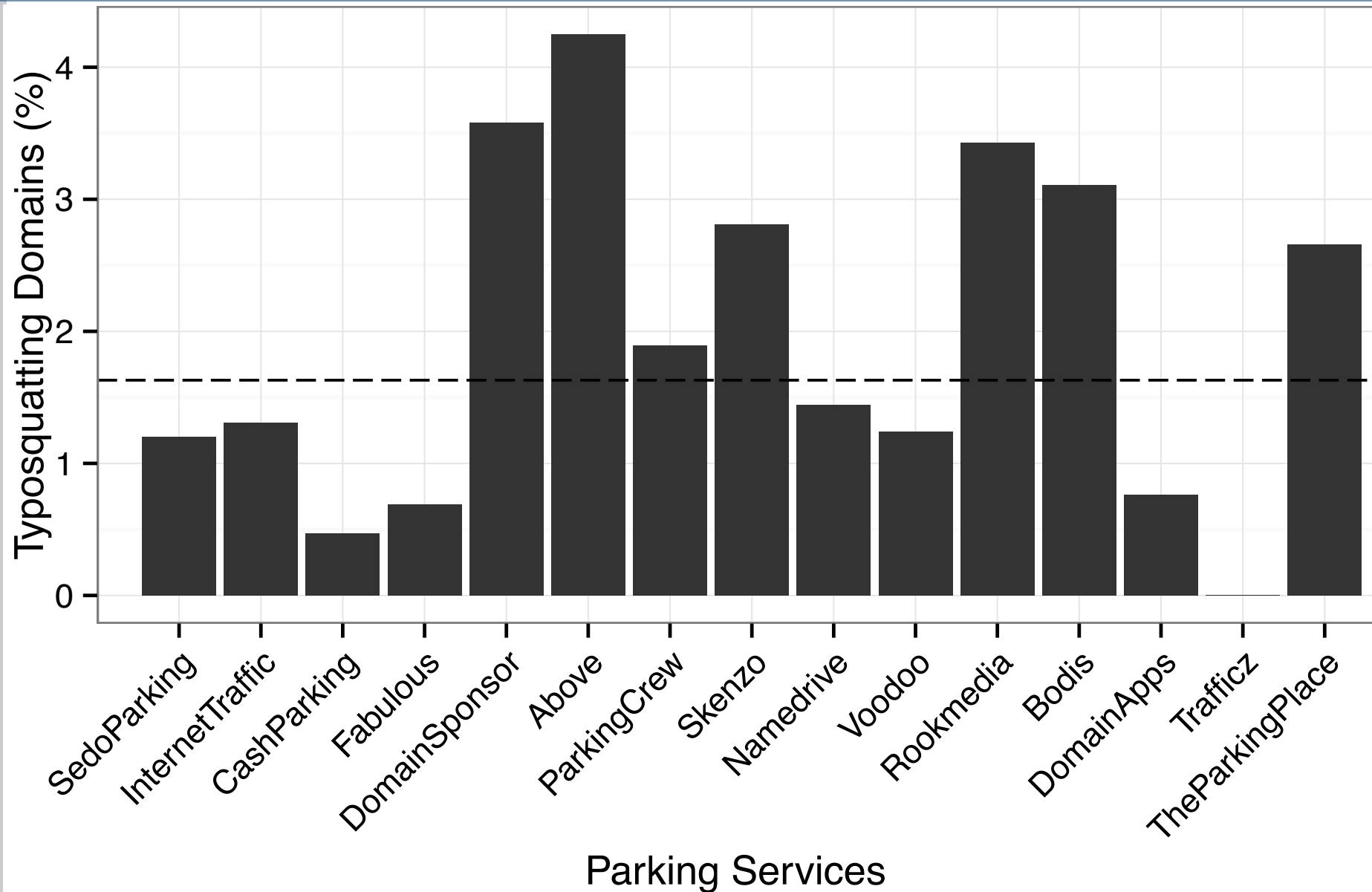
- Data of the large-scale analysis
  - 15 popular domain parking services
    - Alexa, Google, Domaining forum, survey
  - Analyzed 8 million parked domains
    - Found through DNS records
  - Several content-based analyses on samples
    - HTML, frames, HTTP request, screenshot, WHOIS data



# Ecosystem: Parked domains per Parking Service



# Typosquatting abuse: Automated analysis



# Typosquatting abuse: Automated and Manual analysis

- Limitations of automated analysis
  - Trademark abuse
  - Cousin domains (e.g. facebookonline.com)
  - Homophones (e.g. theheneryford.com)
  - No content-based trademark abuse
  
- → Manual analysis of 500 domains
  - 16% abusive domain names
    - 9% typosquatting
    - 7% trademark abuse
  - 37% of abusive domains were displaying ads of a competitor

# Typosquatting abuse: Parking a typo domain

- How “hard” is it to park a typosquatting domain?
- `stackoverflow.com`
- `stcakoverflow.com`
- Attempted to park the domain
  - > Typo Domain was always accepted
  - Even after manual verification by an employee



# Pay-per-Redirection

- Archetypical parked page with PPC ads is not the only monetization strategy
- 7% of visits get redirected to entirely different domains ( = Pay-per-Redirection)
- Often malicious
  - scams, malware, affiliate abuse, adult

# Malicious Redirections: Malware



## Please Install Flash Player Pro To Continue

(Required)

Top Video Sites Require The Latest Adobe Flash Player Update.  
Updating takes under a minute on broadband - no restart is required

### Adobe Flash Player End User License Agreement

This software and other information is delivered to you "as is" and with all faults. Adobe, its suppliers and certification authorities do not and can not warrant the the performance or results you may obtain by using the software, certificate authority services or other third party offerings.

#### 1. Personal Computer Software License Agreement

[Printer-friendly Version](#)


**Accept and Install**

Disclaimer: We are not affiliated nor partnered with Adobe. Adobe has not authored, participated in, or in any way reviewed this advertisement or authorized it. All trademarks, service marks, logos, and/or domain names (including the names of products and retailers) are property of their respective owners. This offering is for a download manager that will install independent 3rd party software that will update the advertised program.

[Privacy Policy](#) · [Terms & Conditions](#) · [Uninstall](#) · [Contact](#)

# Malicious Redirections: Scams

Action Required [Help](#)

✘ Threats Detected

**Threats Detected**

| Title   | Risk     | Status   | Action                          |
|---|----------|----------|---------------------------------|
| <a href="#">Adware.DealPly</a> has been detected. | Critical | Infected | <a href="#">Contact Support</a> |
| <a href="#">Adware.DealPly</a> has been detected. | Critical | Infected | <a href="#">Contact Support</a> |

SYSTEM CRITICALLY INFECTED! CONTACT SUPPORT IMMEDIATELY

Toll Free Helpline : 1866 678 7400

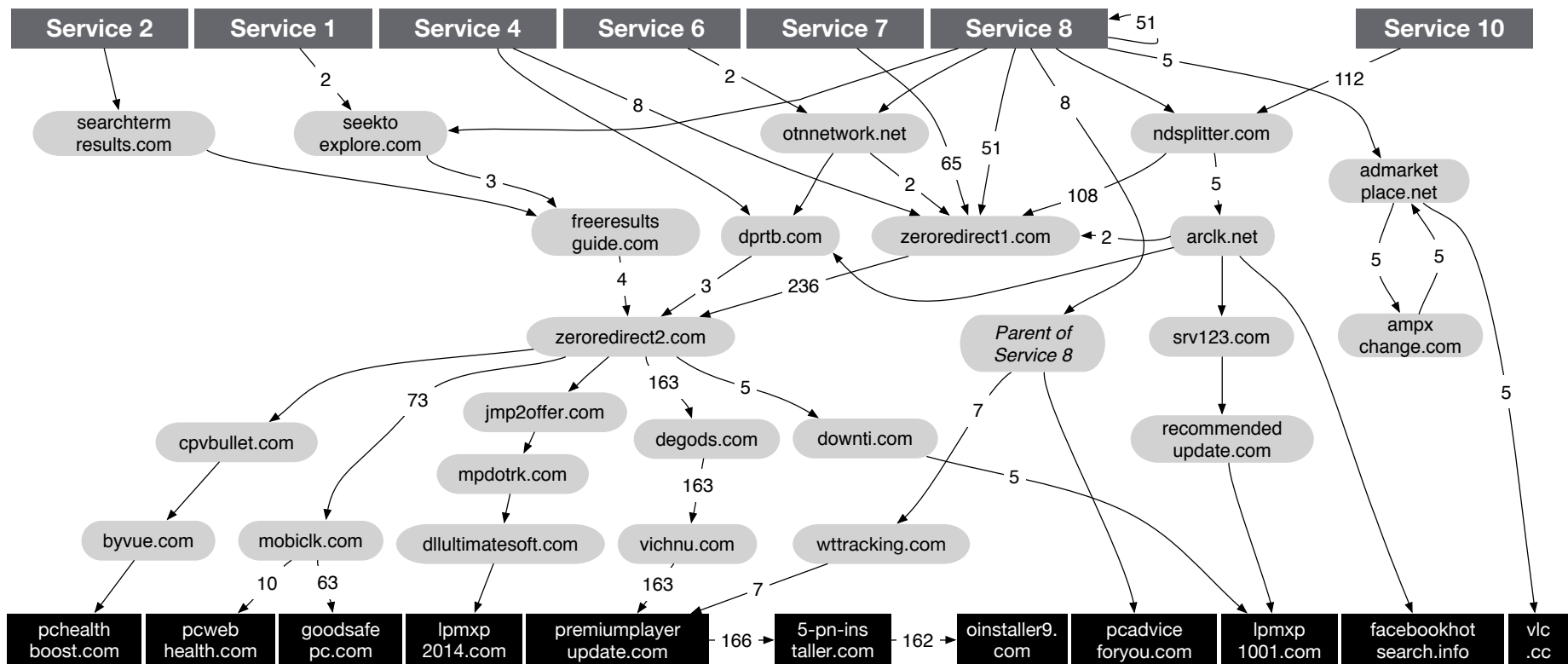
Removed files are quarantined. To restore, [click here](#) \* Recommended Actions

DO NOT TRY TO MANUALLY REMOVE THE VIRUS,  
HARD-DRIVE MIGHT FAIL\*

NORTON TECHNICAL SUPPORT

# Malicious redirections: Redirection chains to malware

- Many parties involved
  - Practices such as *ad arbitration* blur the responsibility





# Malicious redirections

| Service            | United States |         |       |         | Europe       |         |       |         |
|--------------------|---------------|---------|-------|---------|--------------|---------|-------|---------|
|                    | Redirections  | Malware | Scams | Adult   | Redirections | Malware | Scams | Adult   |
| Parking Service 1  | 0.4%          | 66.7%   | -     | -       | -            | -       | -     | -       |
| Parking Service 2  | 1.3%          | 11.1%   | -     | -       | 0.4%         | -       | -     | -       |
| Parking Service 3  | 1.9%          | -       | -     | -       | 2.0%         | -       | 42.9% | 21.4%   |
| Parking Service 4  | 2.6%          | 44.4%   | -     | -       | 3.0%         | -       | -     | 38.1%   |
| Parking Service 5  | 5.0%          | -       | -     | (60.0%) | 5.0%         | -       | -     | (60.0%) |
| Parking Service 6  | 8.6%          | 3.3%    | 21.7% | -       | 2.6%         | -       | -     | (50.0%) |
| Parking Service 7  | 12.4%         | 60.9%   | 1.2%  | -       | 12.0%        | -       | 26.2% | 10.7%   |
| Parking Service 8  | 19.4%         | 42.7%   | 6.6%  | -       | 10.9%        | -       | 26.3% | 2.6%    |
| Parking Service 9  | 34.6%         | 9.1%    | 2.1%  | -       | 34.6%        | 0.4%    | 46.3% | 0.8%    |
| Parking Service 10 | 65.4%         | 21.0%   | 7.4%  | -       | 66.0%        | -       | 54.5% | 27.7%   |

# Detecting Parked Domains

- Parked domains have no added value
  - They're even parasitic and malicious
- Limit exposure to parked domains
- Propose a classifier that is able to detect parked pages
  - Offline: blacklists, search engines,...
  - Online: Browser extensions

# Iterative feature selection

- **Robust features**
  - Does not rely on specifics of parking services
  - Relies on features inherent to the operation of parked domains
- **General focus points**
  - Omnipresence of third-party advertisements
  - Dynamic and on-the-fly page generation
  - Textual content
  - Redirection chains

# Iterative feature selection

- **HTML Features**
  - Average and maximum link length
  - External link and external source ratio
  - Link-to-global text ratio
  - ...
- **HAR Features (some examples)**
  - Third-party HTML content ratio
  - Initial response size and ratio
  - ...
- **Frame Features (some examples)**
  - Main frame and iframe redirections
  - Amount of frames
  - ...

# Detecting Parked Domains: Evaluation

## ■ Dataset

- 3000 parked domains and 3000 non-parked domains
- 2/3 Training set
- 1/3 Test set

## ■ Classifier

- Random-forest
- Feature selection
- Tuning
  - 0.5% False-positive rate
  - 97.9% True-positive rate

# Next steps

- Measure the overhead of feature extraction
- Bias towards archetypical parked pages?
- More studies on Pay-per-Redirection
  - Longitudinal
  - Effect of ad-blockers

# Conclusion

- Insights in domain parking industry and its ecosystem
- Assessed abusiveness and maliciousness
- Proposed a classifier to detect parked pages with minimal false positives.

# Thank you

Thomas Vissers, Wouter Joosen, Nick Nikiforakis

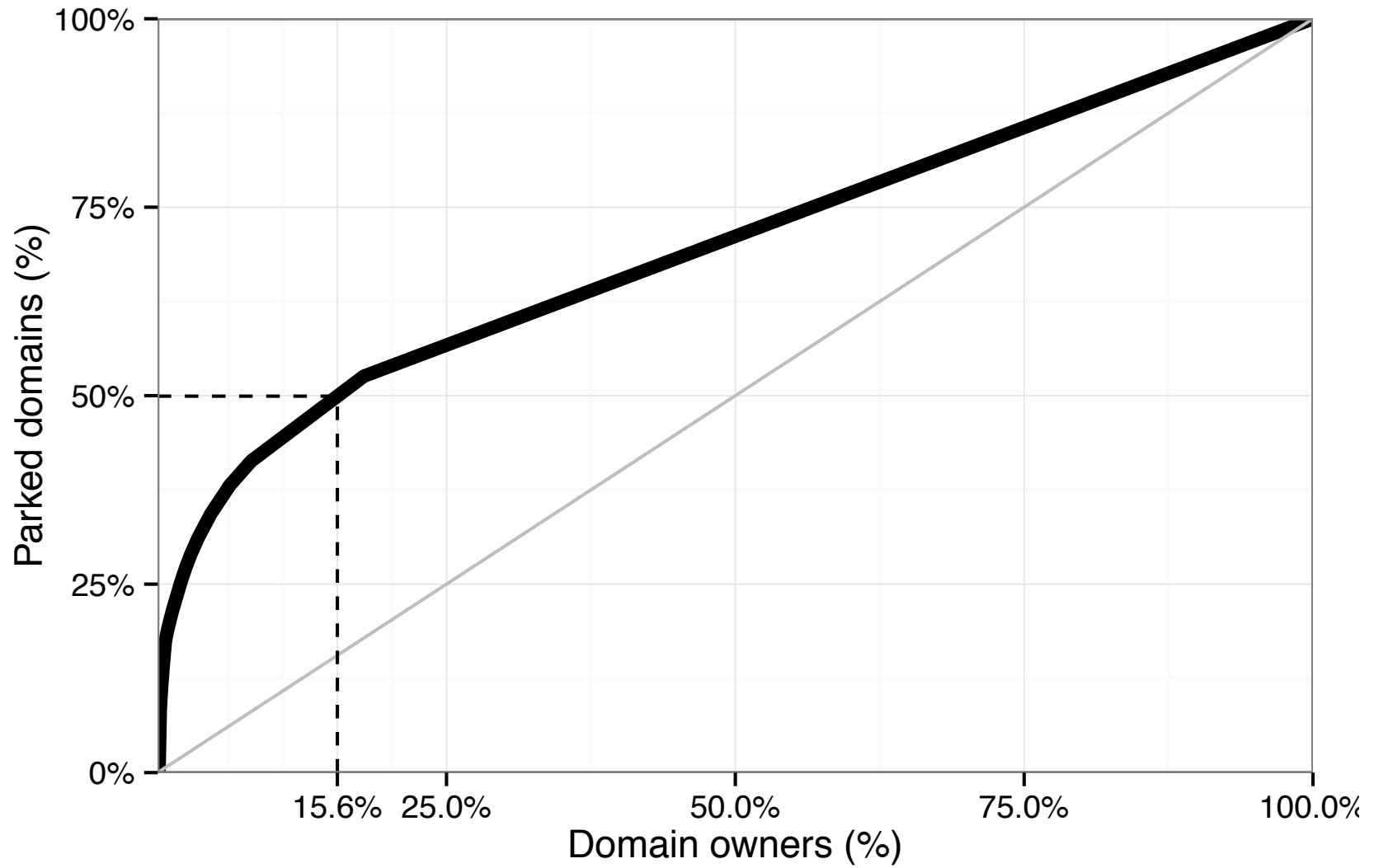


Stony Brook  
University

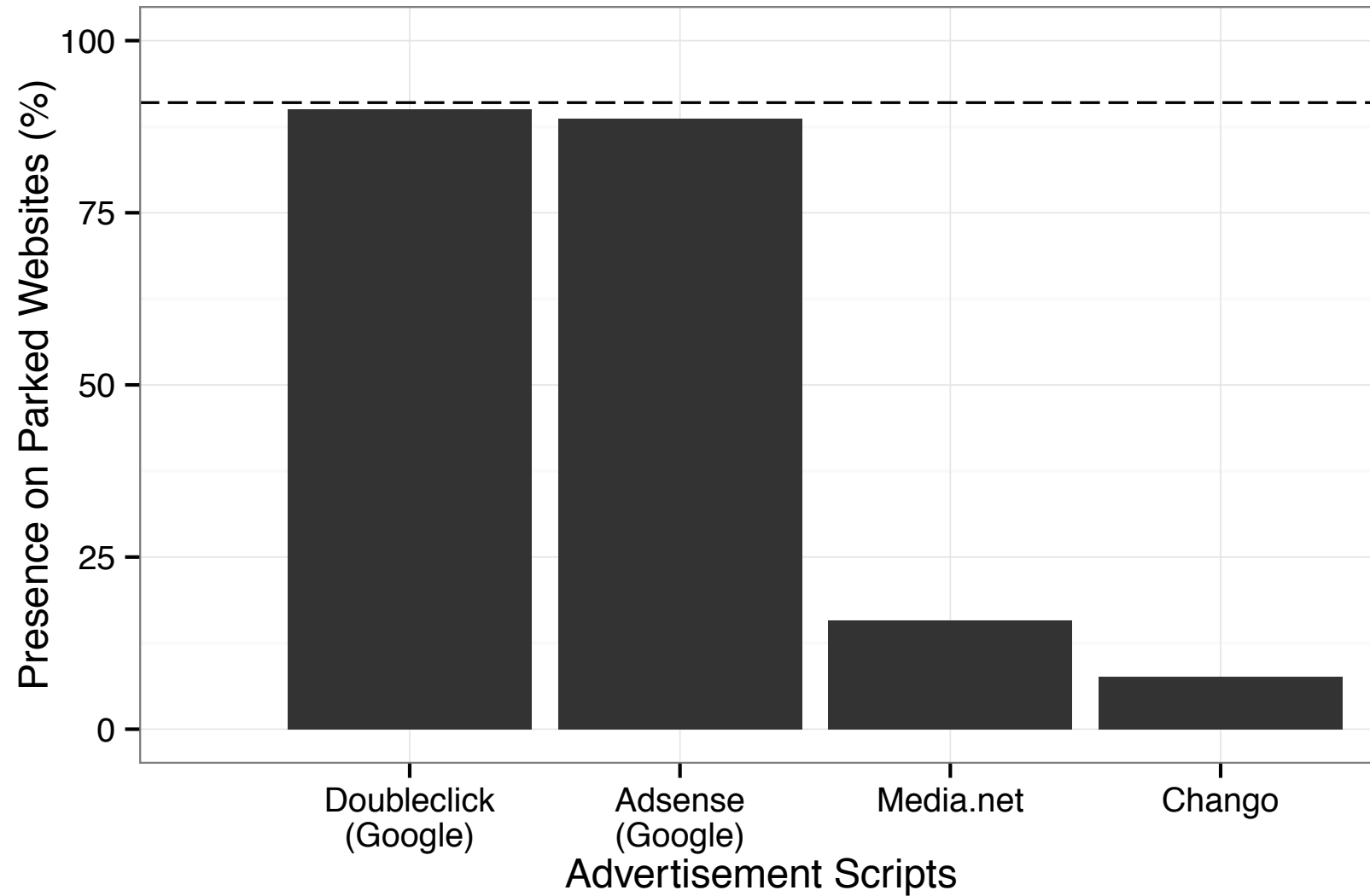


# BACKUP SLIDES

# Domain owners



# 3<sup>rd</sup>-party Ad Syndicators



# ROC Curve detector

