Parking Sensors: Analyzing and Detecting Parked Domains

Thomas Vissers, Wouter Joosen, Nick Nikiforakis
Ecosystem and involved parties

- Domain Owner
- Parking Service
- Advertisement Syndicator
- Advertiser
Ecosystem and involved parties

- Domain Owner
- Parking Service
- Advertisement Syndicator
- Advertiser

Diagram:

1. Domain Owner -> Domain
2. Parking Service -> Domain
3. Advertisement Syndicator -> Domain
4. Advertiser -> Parking Page

Related links:
- AD
- AD
- AD
- AD

Parking Page:
http://www.domain.com
Ecosystem and involved parties

1. Domain

2. Parking Service

3. Advertisement Syndicator

4. Advertiser

Domain Owner
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

- SedoParking
- InternetTraffic
- CashParking
- Fabulous
- DomainSponsor
- Above
- ParkingCrew
- Skenzo
- Namedrive
- Voodoo
- Rookmedia
- Bodis
- DomainApps
- Trafficz
- TheParkingPlace
Typosquatting abuse: Automated analysis

Typosquatting Domains (%)

Parking Services

- SedoParking
- InternetTraffic
- CashParking
- Fabulous
- DomainSponsor
- Above
- ParkingCrew
- Skenzo
- Namedrive
- Voodoo
- Rookmedia
- Bodis
- DomainApps
- Trafficz
- TheParkingPlace
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

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

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

<table>
<thead>
<tr>
<th>Threats Detected</th>
<th>Risk</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware DealFly</td>
<td>Critical</td>
<td>Infected</td>
<td>Contact Support</td>
</tr>
<tr>
<td>Adware DealFly</td>
<td>Critical</td>
<td>Infected</td>
<td>Contact Support</td>
</tr>
</tbody>
</table>

SYSTEM CRITICALLY INFECTED! CONTACT SUPPORT IMMEDIATELY

Toll Free Helpline: 1866 678 7400

Removed files are quarantined. To restore, click here.

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

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

![Graph showing the relationship between domain owners and parked domains. The x-axis represents domain owners (%) ranging from 0% to 100%, and the y-axis represents parked domains (%) ranging from 0% to 100%. The graph illustrates the percentage of parked domains as a function of the percentage of domain owners.]
3rd-party Ad Syndicators

Presence on Parked Websites (%)

Doubleclick (Google) Adsense (Google) Media.net Chango

Advertisement Scripts
ROC Curve detector

False Positive Rate (log scale)

True Positive Rate

90.0%
95.0%
97.9%
98.6%
100.0%