HIDING IN PLAIN SIGHT:
A LONGITUDINAL STUDY OF
COMBOSQUATTING ABUSE

P. KINTIS, N. MIRAMIRKHANI, C. LEVER,
Y. CHEN, R. ROMERO-GÓMEZ, N. PITROPAKIS,
N. NIKIFORAKIS, M. ANTONAKAKIS

OCTOBER 31, 2017
A BRIEF STORY...

- ...it was about a year ago
- Visited nikeshoppings.com
- Bought a pair of shoes for 80€
- Shoes never appeared
- nikeshoppings.com disappeared (!)
IS IT THAT EASY?

455B RRs (30.5TB)

Jan 1, 2011 – Oct 14, 2015
13B RRs (18TB)
discountnikeshopping.com.
flynike.com.
ilovenike.com.
lankanike.com.
lankanikekobe.fr.
nike1000.com.
nikeairxmaxuk.com.
nikeapps.de.
nikecortez.org.
nikecowboyjerseys.com.
nikeelastico.com.
nikees.com.
nikefreerun2016.fr.
nikefreerunpaschere.org.
nikefreerunshoes5.com.
nikelava.com.
nikelebronsoldier10.net.
nikenbahmarkets.com.
nikenenergy.com.
nikenew.fr.
nikeoutletclearancestore.com.
nikes4wholesale.com.
nikeschoenenkopen.nl.
nikestory.com.
niketrainers.com.
niketopanky.net.
nikewear.co.uk.
senikeairmaxrea.se.
wwwfashionnike.blogspot.com.
1-800-806-nike.com.
chaussurenikedunks.com.
chaussurenikeoutletsoldes.com.
cheapnikeairmaxkk.com.
cybermondaynikeshoes.com.
enjoynikerunningtrainersuk.com.
forbiddenluv-nike.blogspot.com.
jp.msn.com.office.nike-poc.myshn.net.
nike-promo-code.com.
nike5666.com.
nike712.net.
nikeairmax90ous.us.
nikespanya.trade.
nikefree2017.se.
nikefree50.fr.
chinanike.cn.
mujer2016nikeairmax.top.
nike3333.com.
nikeaina.com.
nikeairjordans3.site.
nikeairmax2016shoesfr.top.
nikeairmax90-shop.co.uk.
nikeboing.org.
nikebrockosweilerjerseys.com.
nikedomarcuswarejerseys.com.
nikefoot.com.
nikefreerun2016.se.
nikeirelandonline.net.
nikejerseycheapest.com.
nikejerseysbigsale.com.
nikekd8shoes.com.
nikekobe.com.
nikens.com.
nikerunningshoe.com.
nikesbchronicles.com.
nikesbs.com.
nikesize-chart.com.
nikestore.taipei.
nikestorenl.net.
nikesystems.com.
nikeuktrainersshop.com.
sycoairmaxnike.us.com.
nikefreeog.com.
nikefreerunpascherhomme2014.fr.
nikefreerunstore.com.tw.
nikefreerunweb.com.
nikemyadventurecamper.com.
nikeplusapp.com.
nikesairjordanheels.com.
niketrainer1.com.
niketravels.com.
nikevipmall.com.
nikewriteres.com.
pickyanime.com.
nikediscountshoesonlinebuy.com.
nikehyperdunk.org.
nikelaufschuhesaleonline.de.com.
nikelivefabregas.com.
nikeplusbook.com.
COMBOSQUATTING DEFINITION

Before we continue...

^[a-zA-Z0-9]*

• Must contain the trademark intact
• Must not be typosquatting
TRADEMARKS

- 268 trademarks
- 22 categories
• Combosquatting domains in different business categories
• Thousands of combosquatting domains for many trademarks
• Active combosquatting domain names over almost six years
• Static number of domain names resolved
• Increasing trend in domain name registrations over time
## COMBOSQUATTING DNS DATASETS

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Count</th>
<th>Time Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>•</td>
<td>2,321,914</td>
<td>Jan 2011 – Oct 2016 1.1B</td>
</tr>
<tr>
<td>Active</td>
<td>•</td>
<td>1,022,083</td>
<td>Dec 2012 – Sep 2016 610M</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>9,283</td>
<td>Oct 2008 – Nov 2016 22K</td>
</tr>
<tr>
<td></td>
<td>PBL</td>
<td>3,750</td>
<td>Jul 2009 – Sep 2016 966K</td>
</tr>
<tr>
<td></td>
<td>Spam</td>
<td>2,296</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APT</td>
<td>59</td>
<td></td>
</tr>
</tbody>
</table>

### Combosquatting DNS Datasets

- **Passive:** 2,321,914
- **Active:** 1,022,083

### Categories:

- **Malware:**
  - Count: 9,283
  - Size: 1.1B

- **PBL:**
  - Count: 3,750
  - Time: Dec 2012 – Sep 2016
  - Size: 610M

- **Spam:**
  - Count: 2,296
  - Time: Jul 2009 – Sep 2016
  - Size: 966K

- **APT:**
  - Count: 59
  - Size: 22K
PHISHING ATTACKS

bankofamerica-com-login-sys-update-online.com
SOCIAL ENGINEERING ATTACKS

airbnbforbeginners.com
TIP OF THE ICEBERG

- activatemycrbankofamerica.com
- activatemycrebankofamerica.com
- activatemycredbankofamerica.com
- activatemycredibankofamerica.com
- activatemycreditbankofamerica.com
- activatemycreditcabankofamerica.com
- activatemycreditcarbankofamerica.com
- activatemycreditcardbankofamerica.com
Domain name resolutions by clients in North America
IN X.509 WE TRUST

• 691,182 TLS certificates
• 107,572 combosquatting FQDNs
knowledge [nol-ij] facts, information, and skills acquired by a person through experience or education;

Synonyms: cognition, information, acquaintance, developmental activity...
LEXICAL CHARACTERISTICS

![Graph 1: CDF of Length Frequency](image1)

![Graph 2: CDF of Volume Frequency](image2)
COMBOSQUATTING ANALYSIS

Init
• Start with 1.3M combosquatting domains from the Active DNS dataset

Affiliate Abuse
• Redirection through affiliates
  • 2,573 domains

Phishing
• Found 40K domains with login forms
  • Manually identified 174 unique phishing pages

Processing
• Selected the most popular domains
  • Created clusters and labeled 8.7K domains

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>86.6%</td>
</tr>
<tr>
<td>Malicious</td>
<td>13.39%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrelated</td>
<td>11.23%</td>
</tr>
<tr>
<td>Suspicious</td>
<td>88.77%</td>
</tr>
<tr>
<td>Phishing</td>
<td>0.9%</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>13.62%</td>
</tr>
<tr>
<td>Affiliate Abuse</td>
<td>15.56%</td>
</tr>
<tr>
<td>Trademark Abuse</td>
<td>69.9%</td>
</tr>
</tbody>
</table>
The Chevron Case
• Registrants
  • Defensive registrations (very hard)
  • Do not use your trademark in new domains for campaigns (paypal-prepaid[.]com)
• Registrars
  Flag domains that contain popular trademarks
  Request verification and hand-verify the registration request
• Third Parties
  • Domain analysis systems should take combosquatting into consideration
REGISTRARS TAKING ACTION

This domain contains restricted phrase(s) and can’t be self registered. Please contact our support to see if we can register it for you manually.

facebook-login.store  SPECIAL
facebook-login.world  SPECIAL
facebook-login.me  SPECIAL

twitter-login.store  SPECIAL
$4.88/year
Retail $48.88/year

twitter-login.world  SPECIAL
$1.88/year
Retail $24.88/year

twitter-login.me  SPECIAL
$2.88/year
Retail $18.99/year
Equifax Hack 2017: Which Equifax Site Is Fake?

William White  
InvestorPlace  September 21, 2017

The saga of the Equifax Inc. (NYSE: EFX) hack continues with more blunders from the company.
How were we still able to do this?
Why haven’t you learned anything?
THANK YOU!

PANAGIOTIS KINTIS
KINTIS@GATECH.EDU