WHEN COMBOSQUATTING IS THE FIRST HOOK

PANAGIOTIS KINTIS
SEPTEMBER 27, 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 (!)
455B RRs (30.5TB)

Jan 1, 2011 – Oct 14, 2015
13B RRs (18TB)
COMBOSQUATTING DEFINITION

Before we continue...

^[a-zA-Z0-9-]* [a-zA-Z0-9-]*

- Must contain the trademark intact
- Must not be typosquatting
CAN WE FIND MORE?

- Obtained the 500 most popular domain names
- Removed domains that could induce noise
  - Apple
  - AT&T
  - Bing
  - IKEA
  - ...
- Created a list of “trademarks” we would study
• 268 trademarks
• 22 categories
Combosquatting domains in different business categories
Active combosquatting domain names over almost six years
COMBOSQUATTING DNS DATASETS

- Passive: 2,321,914
- Active: 1,022,083
- Malware: 9,283, 6,886
- PBL: 3,750, 4,787
- Spam: 2,296, 6,400
- APT: 59, 56
PHISHING ATTACKS

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

Your version of Flash Player might be outdated.

Updates are ready to install.

Copyright © 2005 Adobe Systems Incorporated. All rights reserved.

airbnbforbeginners.com
TIP OF THE ICEBERG

- activatemycrbankofamerica.com
- activatemymeabankofamerica.com
- activatemycrdibanofamerica.com
- activatemycrbkbankofamerica.com
- activatemycrdibankofamerica.com
- activatemycrditbankofamerica.com
- activatemycrditcabanofamerica.com
- activatemycrditcarbankofamerica.com
- activatemycrditcardbankofamerica.com
Sometimes people are just...
Domain name resolutions by clients in North America
INFRASTRUCTURE DIVERSITY
IP CHARACTERISTICS

- CDF of Number of IP Addresses
- CDF of Domain Names per IP
- CDF of Domain Lifetime

Georgia Tech

CREATING THE NEXT®
POPULARITY

CDF

Lookup Volume (per Domain)

Domain Name Resolutions

Lookup Volume

Date

ComodoSquatting
Malicious

ComodoSquatting
Malicious

10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9 10^10 10^11

10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9 10^10 10^11

10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9 10^10 10^11

10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9 10^10 10^11

2011 2012 2013 2014 2015
PERSISTENCE
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, especially
### 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>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unknown</strong></td>
<td>86.6%</td>
</tr>
<tr>
<td><strong>Suspicious</strong></td>
<td>88.77%</td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
<td>0.9%</td>
</tr>
<tr>
<td><strong>Social Engineering</strong></td>
<td>13.62%</td>
</tr>
<tr>
<td><strong>Affiliate Abuse</strong></td>
<td>15.56%</td>
</tr>
<tr>
<td><strong>Trademark Abuse</strong></td>
<td>69.9%</td>
</tr>
<tr>
<td><strong>Malicious</strong></td>
<td>13.39%</td>
</tr>
<tr>
<td><strong>Unrelated</strong></td>
<td>11.23%</td>
</tr>
</tbody>
</table>
BUSINESS CATEGORIES AFFECTED

- Adult Content
- Blogging
- Computers
- Radio & TV
- E-Learning
- Lifestyle
- News
- Couriers
- E-Shop (C2C)
- Photography
- Search Engines
- Social Networks
- Software & Web
- Streaming
- Telecom
- Travel

Trademark Abuse

- E-Shop (Online): 61.65%
- E-Shop (Physical): 72.5%

Affiliate Abuse

- Financial: 55.11%
- File Sharing: 51.35%

Social Engineering

Attention BANK OF AMERICA Visitor

Bank of America would like all New York residents to complete a short survey because we are committed to making sure that all of our customers receive the highest quality service.

To say Thank You we have selected a range of high quality Free Gifts worth over $500 for you to choose from.

Continue
REDIRECTION GAMES (HUMAN DRIVEN)

- User sits in front of the computer and visits websites
- Redirection can go to either a random page or to malware related pages

Flowchart:
- User
- Website Visited: zillowhomesforsale[.]com, youtubezeeneletoltes[.]com
- Real User
- YES: Malware
  - http://www.searchnet[.]com/Search/Loading?v=5 or FlashPlayer.dmg
- NO: Dummy Page
  - Parking Social Engineering
• Visiting domains with no HTTP “User-Agent” header information results in a parking page
• Visiting domains with HTTP header information will result in a probabilistic redirection

• starbucksben[.]com → ww1.starbucksben.com
• http://zillowhomesforsale[.]com/ →
  http://rtbtracking[.]com/click?data=Mm[...Q2&id=8c[...]d3
User (1) -> Website Visited

- jcpennyoutlet[.]com
- toysrusuk[.]com
- expediancredit[.]com
- nordstrombenefits[.]com

Set Cookie -> admarketplace[.]net

Set Cookie -> Set Cookie

(2)

ampingexchange[.]com

Set Cookie

(3)

First Visit

YES -> Affiliate Page

NO -> Dummy Page

(4)

jcpenney[.]com
target[.]com
 nordstrom[.]com

(5)

Parking
Social Engineering
theclickcheck[.]com

EXAMPLE
THE CHEVRON CASE

- Visiting chevrontexacobusinescard[.]com has two potential outcomes
  - A parking page of no interest
  - A redirection through obfuscated JavaScript
CAN WE SOLVE THE PROBLEM?

• 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
THE EQUIFAX CASE

Equifax Hack 2017: Which Equifax Site Is Fake?

The saga of the Equifax Inc. (NYSE:EFX) hack continues with more blunders from the company.

Aug 22

Sep 8
HOW CAN I HELP?

• Do you have domain names?
• Do you have your own DNS data?
• Do you want us to run our algorithms on your datasets?
• Do you want to help the Active DNS Project?
• Do you want to give us some feedback? 😊
EXPLOITING COMBOSQUATTING
THANK YOU!

PANAGIOTIS KINTIS
KINTIS@GATECH.EDU