FACEBOOK OSINT
ITS FASTER THAN SPEED DATING

17 October 2013 | HITB2013KUL
Keith Lee
Jonathan Werrett
INTRODUCTION

Keith Lee
Security Analyst, SpiderLabs, Singapore
klee@trustwave.com
http://github.com/milo2012/osintstalker
@keith55

Jonathan Werrett
Managing Consultant, SpiderLabs, Hong Kong
jwerrett@trustwave.com
@werrett
AGENDA

‣ Background / Motivation
‣ Introduction to GeoStalker and FBStalker tools
‣ Problem they solves
‣ GeoStalker in-depth
‣ FBStalker in-depth
‣ What you can do to protect yourself
MOTIVATION

Spend our days on “Penetration tests”

Web apps and networks

Day-in day-out
MOTIVATION

Spend our days on “Penetration tests”

Web apps and networks

Day-in day-out
Some times we get a real pentest

Set specific targets

Gain access any way you can

...
Some times we get a real pentest
Set specific targets
Gain access any way you can

...
**GEOSTALKER**

Takes

- Location (address or coordinates)

Retrieves location data from

- Wigle.net (Wireless DB)
- Instagram
- Twitter
- Foursquare
- Flickr

Provides

- Wireless access points near-by
- Photos taken at that location
- Social media accounts of people who’ve visited

**FBSTALKER**

Takes

- Facebook profile user

Uses Graph Search to reverse

- Friends
- Likes
- Check-ins
- Comments

Provides

- Social engineering targets
- Associates of those targets
- Times online
- Interests, commonly visited places
EXAMPLE OBJECTIVES

- **Premise Recon?**
  - Google Maps
  - Geocode Lat / Lon
  - Staff

- **Phishing Targets?**
  - Physical Address
  - Geocode Lat / Lon
  - Twitter, Instagram, 4sq, Flickr

- **LinkedIn, Facebook**

- **Entry Points**
  - Photos

- **Facilities**
  - Staff

- **Staff**

- **Interests**
  - Associates
EXAMPLES FROM ENGAGEMENTS
EXAMPLES FROM ENGAGEMENTS

FB Apps

- Indicate phishing target uses mac
- Ditch our Windows based payloads for OSX
EXAMPLES FROM ENGAGEMENTS

FB Apps
- Indicate phishing target uses mac
- Ditch our Windows based payloads for OSX

FB Friends
- Identify targets wife
- Wife runs Pilates studio
- Spear phish wife based on Pilates
EXAMPLES FROM ENGAGEMENTS

FB Apps
- Indicate phishing target uses mac
- Ditch our Windows based payloads for OSX

FB Friends
- Identify targets wife
- Wife runs Pilates studio
- Spear phish wife based on Pilates

Instagram Photos
- Client was a power utility
- Staff target found via on photos from facilities
GEOSTALKER - INTRO

Requires

- Address
- Latitude / Longitude Coordinates

Queries sources

- Wigle.net (Wireless DB)
- Instagram
- Twitter
- Foursquare
- Flickr

Provides

- Wireless devices
- Photos
- Social network accounts
- Searches social network accounts for ‘like’ names
DEMO

GEOSTALKER
Please enter an address or GPS coordinates (e.g. 4.237588,101.131332): 1.358143,103.944826
Geostalker - Running

******************************************************************************
***** Geostalker Version 1.0 HackInTheBox Release *****
******************************************************************************

Please enter an address or GPS coordinates (e.g. 4.237588,101.131332): 1.358143,103.944826
[*] Converting address to GPS coordinates: 1.358143 103.944826
[*] Downloading Wige database from Internet
[*] Wige database already exists: 1.358143_103.944826.dat
[*] Checking Google Docs if File Exists
[*] Logging in... Login success!
[[ File: 1.358143_103.944826.kml exists!
[*] Change: 1.358143_103.944826.kml Access to Public
[*] Logging in... Login success!
owner user testosint1@gmail.com
reader default None
Permissions change success!
[*] Extracting MAC addresses from Wige database: 1.358143_103.944826.dat
[*] Retrieving match for vendor name: TP-LINK TECHNOLOGIES CO., LTD.
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: 2wire
[*] Retrieving match for vendor name: Cisco-Linksys LLC
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Aztech Electronics Pte Ltd
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: TP-LINK TECHNOLOGIES CO., LTD.
GEOSTALKER - RUNNING

[*] Downloading Instagram Data based on Geolocation
[*] Found http://instagram.com/valarieong (1.353651352, 103.947589982)
[*] Found http://instagram.com/the__wilson (1.35708421, 103.946482756)
[*] Found http://instagram.com/qkserene (1.35380119, 103.94755082)
[*] Found http://instagram.com/jolenengg (1.356181544, 103.944273863)
[*] Found http://instagram.com/cakebaya (1.356661622, 103.946155753)
[*] Found http://instagram.com/mdsf134 (1.3585548, 103.9459623)
[*] Found http://instagram.com/staticattack7 (1.366655809, 103.959112024)
[*] Found http://instagram.com/zeslablaza (1.3538664, 103.95066925)
[*] Found http://instagram.com/lionrawrs (1.35444817, 103.94413959)
[*] Found http://instagram.com/syhrh (1.35508942, 103.948095805)
[*] Found http://instagram.com/_tinc (1.35965, 103.949211667)
[*] Found http://instagram.com/staticattack7 (1.36678, 103.95011)
[*] Found http://instagram.com/_juicebox (1.354171506, 103.945883532)
[*] Found http://instagram.com/justjiro (1.363914386, 103.953111302)
[*] Found http://instagram.com/susan_wong (1.358982817, 103.936833669)
[*] Found http://instagram.com/leo1992430 (1.354916, 103.9507291)
[*] Found http://instagram.com/victorhooi (1.35653, 103.9441)
[*] Found http://instagram.com/slyj91 (1.354752627, 103.939547539)
[*] Found http://instagram.com/careyblue21 (1.355752622, 103.941212641)
[*] Found http://instagram.com/nashrfredhilton (1.357772, 103.947368)
[*] Found http://instagram.com/jacquiskyl (1.3529967, 103.9486539)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567486, 103.9472094)
[*] Found http://instagram.com/sna1lvhi_tesingapore (1.352943594, 103.93902806)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567597, 103.9471805)
[*] Found http://instagram.com/abelspears (1.352668869, 103.944063542)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567204, 103.9472365)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567208, 103.9473055)
[*] Found http://instagram.com/conxtaxxx (1.355943009, 103.942008859)
[*] Found http://instagram.com/shannonsohh (1.3595, 103.948166667)
[*] Found http://instagram.com/xiaooxuann (1.360759293, 103.95300796)
[*] Found http://instagram.com/salihayourbabygurl (1.354260869, 103.951874971)
[*] Found http://instagram.com/syhrh (1.353779637, 103.943580469)
[*] Found http://instagram.com/staticattack7 (1.36678, 103.95011)
[*] Found http://instagram.com/yonkizeyyy (1.36642948, 103.946193808)
[*] Found http://instagram.com/frrnhh_ (1.3566542, 103.9460857)
[*] Found http://instagram.com/jannynarma (1.35605193, 103.9441048)
[*] Found http://instagram.com/syhrh (1.354931434, 103.947560092)
[*] Found http://instagram.com/friendlyweirdo (1.367884449, 103.950825054)

[*] Downloading Flickr Data based on Geolocation
[*] Continue Downloading Flickr Data
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address 1</th>
<th>IP Address 2</th>
<th>Company Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3C:EA:4F:5E:13:71</td>
<td>1.35665429</td>
<td>103.94688786</td>
<td>2Wire</td>
<td></td>
</tr>
<tr>
<td>C0:C1:C0:22:70:EA</td>
<td>1.35664415</td>
<td>103.94662476</td>
<td>Cisco-Linksys, LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>64:0F:28:4E:9B:42</td>
<td>1.3567121</td>
<td>103.94638024</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:18:39:A3:2F:60</td>
<td>1.3563722</td>
<td>103.94682143</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>64:0F:28:4A:7F:AE</td>
<td>1.3564880</td>
<td>103.94675546</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>98:2C:BE:15:CF:82</td>
<td>1.3564712</td>
<td>103.94682143</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>F4:EC:38:AD:3B:B4</td>
<td>1.3567121</td>
<td>103.94638024</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:13:18:2F:8B:6B</td>
<td>1.3566323</td>
<td>103.94677734</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:1F:B3:63:81:69</td>
<td>1.35653831</td>
<td>103.94632721</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:1F:B3:63:81:69</td>
<td>1.35653831</td>
<td>103.94632721</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>8B:EC:75:4F:6F:C9</td>
<td>1.3565429</td>
<td>103.94688786</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>64:0F:28:47:1E:BA</td>
<td>1.3564880</td>
<td>103.94675546</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:0F:6F:2F:48:5B</td>
<td>1.3565429</td>
<td>103.94688786</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>34:EF:44:79:8C:39</td>
<td>1.35664713</td>
<td>103.94671631</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:28:75:57:4E:7B</td>
<td>1.35649908</td>
<td>103.94627380</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
<tr>
<td>00:12:17:0F:69:05</td>
<td>1.3565429</td>
<td>103.94688786</td>
<td>Cisco-Linksys LLC</td>
<td>2Wire</td>
</tr>
</tbody>
</table>

**TOTAL**: 103.94688786 meters
[*] Searching for valid accounts: https://www.facebook.com/victorhooi

[*] Searching for valid accounts: https://www.youtube.com/user/victorhooi/feed

[*] Found: https://www.youtube.com/user/victorhooi/feed

[*] Searching for valid accounts: http://instagram.com/victorhooi

[*] Searching for valid accounts on Google+

[*] Searching Google+ for Possible Matches: victorhooi

[*] Searching for valid accounts on Linkedin

[*] Searching on Linkedin for: victorhooi

[*] Searching for valid accounts on Google Search

[*] Searching for valid accounts: https://www.facebook.com/slyj91

[*] Searching for valid accounts: https://www.youtube.com/user/slyj91/feed

[*] Searching for valid accounts: http://instagram.com/slyj91

[*] Searching for valid accounts on Google+

[*] Searching Google+ for Possible Matches: slyj91

[*] Searching for valid accounts on Linkedin

[*] Searching on Linkedin for: slyj91
GEOSTALKER - FOURSQUARE
GEOSTALKER - INSTAGRAM

http://instagram.com/thisisisu
1.355188333,103.944221667
1.358143
GEOSTALKER - FLICKR
GEOSTALKER - HTML OUTPUT
GEOSTALKER - MALTEGO EXPORT
GEOSTALKER - LIMITATIONS

Single threaded

Query by GPS location or address only
GEOSTALKER - FUTURE VERSIONS

Multithreaded - Run faster!

Extend Maltego Mgtx export

Allow to disable specific datasource
FBSTAKLER - INTRO

Requires

- Profile Name

Graph Search to find

- Friends
- Likes
- Check-ins
- Comments

Provides

- Reverse engineered friend list
- Strength of associations
- Regular posting time (wake time?)
FBSTALKER - LOCKDOWN VS NON-LOCKDOWN

Lockdown Profile

‣ Unable to see the list of friends
‣ Reverse engineer the list of friends from likes and tags

Open Profile

‣ Analyze all friends of target and determine how two individuals are connected or know each other.
  ‣ Work place
  ‣ School
  ‣ Common interests
  ‣ Common friends
  ‣ Places that two individuals like
FACEBOOK GRAPH KEYWORDS
UNDERSTAND HOW 2 INDIVIDUALS ARE CONNECTED / RELATED
FBSTALKER - GRAPH SEARCH EXAMPLE
FBSTALKER - GRAPH SEARCH EXAMPLE
FBSTALKER - INPUT

FLD-SP-C02HJ: test klee$ python2.6 fb_test2.py -user joesullivan
[*] Username: joesullivan
[*] Uid: 733651102

[*] Writing 1 record(s) to database table: videosBy
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: DallasCAC
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: DallasCAC
[*] Extracting Data from Photo Page: flexengineer
[*] Extracting Data from Photo Page: tomw
FBSTALKER - RUNNING

********** Places Visited By joesullivan **********
Public Places & Attractions: Gym   UCSF Mission Bay Conference Center https://www.facebook.com/UCSFMissionBayConferenceCenter
Hotel    Sheraton Dallas https://www.facebook.com/SheratonDallas
Event    Catamaran Resort Luau https://www.facebook.com/CatamaranResortLuau
Corporate Office: Campus Building   Facebook HQ https://www.facebook.com/pages/Facebook-HQ/166793020034304
Corporate Office  Google CLS https://www.facebook.com/pages/Google-CLS/121693884547086
Park      Greer Park https://www.facebook.com/pages/Greer-Park/11257685464637

********** Places Liked By joesullivan **********

********** Places checked in **********
2013-02-13 00:20:11   The Facebook Suite at the Center, University of Alabama Birmingham https://www.facebook.com/pages/The-Facebook-Suite

********** Apps used By joesullivan **********

********** Videos Posted By joesullivan **********
https://www.facebook.com/photo.php?v=10100609712053311  What most schools don’t teach

********** Pages Liked By joesullivan **********

********** Friendship History of joesullivan **********

*** Backtracing from Facebook Likes/Comments/Tags ***
boz
maryp
charlotte
larrymagid
marisa.fagan
twt
christian.p.sullivan
jack.christin
davidreccordon
sacredheartsCS
LiveNationBayArea
traci.holdt
zuck
pondhockeymovie
tim.gould.1029
dustin
Palo Alto Police
adamconner
97896471439

Thursday, 17 October 13
FBSTALKER - PROBLEMS

Facebook Graph API is limited

PhantomJS had some issues with Facebook site

Had to use Chromedriver

Single threaded
FBSTALKER - FUTURE WORK

- Runs 100% headless
- Monitor changes / activities of user’s FB profile.
- Allow name as input instead of userid
- Point system for Association strength
  - Photo Tags
  - Check-ins
  - Comments
  - Post / Photo Likes
HOW TO PROTECT YOURSELF

Turn off ‘location’ setting in social networking apps

Tighten Facebook privacy settings

AVG PrivacyFix

RECLAIM PRIVACY.ORG