

Using Social Networks to Find, Profile and Own Your Victims!



@DaveMarcus

Director Security Research, McAfee Labs

Founding Keyholder

Unallocated Space

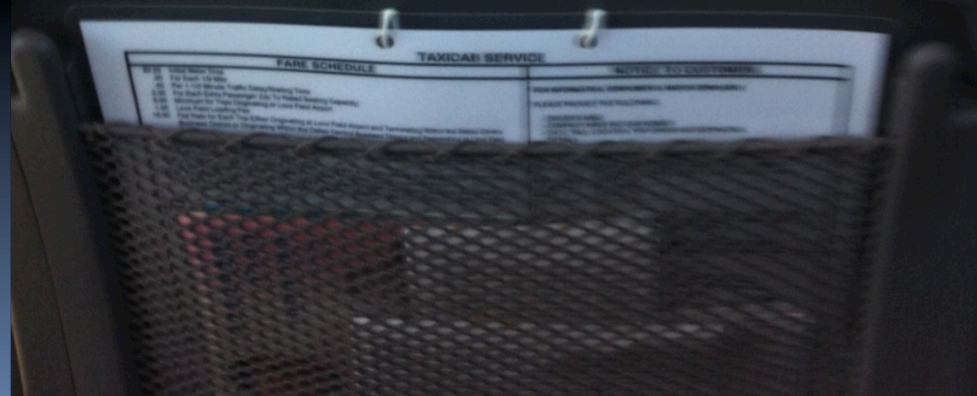
A Maryland Hackerspace

Maryland TOOOOL Headquarters

Learn. Teach. Party.

WARNING

The method used to authenticate credit card transactions for approval is not secure and personal information is subject to being intercepted by unauthorized personnel.





Agenda

- Privacy
- Open Source Intelligence
- Profiling, pownage and ownage

Privacy – Yeah Right

- Zero History is Impossible
- Overshare
- Data Permanence
- Using OSINT

What is OSINT?

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or classified sources); it is not related to open-source software or public intelligence.

Wikipedia Definition

Forms of OSINT

OSINT includes a wide variety of information and sources:

- * Media: newspapers, magazines, radio, television, and computer-based information.
- * Web-based communities and user generated content: social-networking sites, video sharing sites, wikis, blogs, and folksonomies.
- * Public data: government reports, official data such as budgets, demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements and contract awards.
- * Observation and reporting: amateur airplane spotters, radio monitors and satellite observers among many others have provided significant information not otherwise available. The availability of worldwide satellite photography, often of high resolution, on the Web (e.g., Google Earth) has expanded open source capabilities into areas formerly available only to major intelligence services.
- * Professional and academic: conferences, symposia, professional associations, academic papers, and subject matter experts.

Wikipedia Definition

Our Needed OSINT Toolset

- We need a tool to mine the data, trends and topics that our victims are talking about
- PicFog - Images
- Mine Twitter, LinkedIn, Digg, etc...
- We need these tools for “FREE”

Good Reconnaissance Pays Dividends

Finding Open Source Intelligence In Social Media and Networks

The image is a collage of social media profiles and search results for Dave Marcus. At the top left is a Twitter profile for Dave Marcus (@DaveMarcus), Director of McAfee Labs Security Research Communications, with a bio that says "RIGHT BEHIND YOU!!!". To the right is a LinkedIn profile for Dave Marcus, Account Type: Basic, with navigation links for Home, Profile, Contacts, Groups, Jobs, Inbox (42), and Company. Below these is a Facebook profile for Dave Marcus, with a News Feed and Messages section. The central focus is a Twitter search results page for "from:davemarcus", showing three tweets. The first tweet is a retweet of @twisterdavemd, mentioning a tool for finding physical locations from Twitter names. The second tweet is a retweet of @bobmcmillan, mentioning a book "When Gadgets Betray Us". The third tweet is from @theprez98, mentioning a tool. The date "June 23, 2011" is visible at the bottom right of the collage.

Dave Marcus
@DaveMarcus RIGHT BEHIND YOU!!!
Director of McAfee Labs Security Research Communications
<http://www.avertlabs.com/research/blog>

Linked in Account Type: Basic
Home Profile Contacts Groups Jobs Inbox 42 Company
Are You A Director? - Apply to Cambridge W...
Edit Profile View Profile

facebook
Dave Marcus
Edit My Profile
News Feed
Messages

twitter from:davemarcus Search
Results for from:davemarcus 0.06 seconds

DaveMarcus: RT @twisterdavemd: @DaveMarcus find a person's physical location with only their Twitter name. <http://bit.ly/hlOznD> (expand) < yeppers! great tool! less than 20 seconds ago via TweetDeck · Reply · View Tweet

DaveMarcus: RT @bobmcmillan: Got my copy of @robertvamosi 's When Gadgets Betray Us. Looks very interesting. <http://mcaf.ee/1fa3c> < an excellent read!+1 11 minutes ago via TweetDeck · Reply · View Tweet

DaveMarcus: @theprez98 have had it for a while.... quite handy! about 2 hours ago via TweetDeck · Reply · View Tweet · Show Conversation

June 23, 2011



The Strange Case of Dan Redux.....

[Redacted]

Senior Natural Search Analyst at iCrossing

Brighton, United Kingdom | Online Media

Current

- Senior Natural Search Analyst at iCrossing

Past

- Search Engine Analyst at Spannerworks
- Web Developer at parenta

Education

- University of Greenwich
- University of Greenwich

Recommendations

1 person has recommended Dan

Connections

145 connections

Websites

- Search Engine Optimisation
- My Twitter Feed

Twitter

[Redacted]

Public Profile

[http://uk.linkedin.com/in/\[Redacted\]](http://uk.linkedin.com/in/[Redacted])

- [do DS Blog](#)
- [file](#)
- [file](#)
- [Profile](#)
- [- Skate at Night](#)
- [ofile](#)

ed on Google
at works

Design, Flatland BMX,

A
In
he
O
ga
W
Si
PI
Br
C
iCrossing Spannerworks

Jan 20, 2011 09:16 AM GMT - via Destroy Twitter · Reply · View Tweet

- Islandia
- Razzie
- Jav Cutler

1 Daniel [Redacted] Age: 30
[Redacted], Brighton, [Redacted], [Redacted]

View Address



@handolio If i can't do Saturday I'll be up for probably a shorter ride Sunday, I should know later today whether I can do Saturday.
Jan 19, 2011 09:16 AM GMT - via Destroy Twitter · Reply · View Tweet · Show Conversation

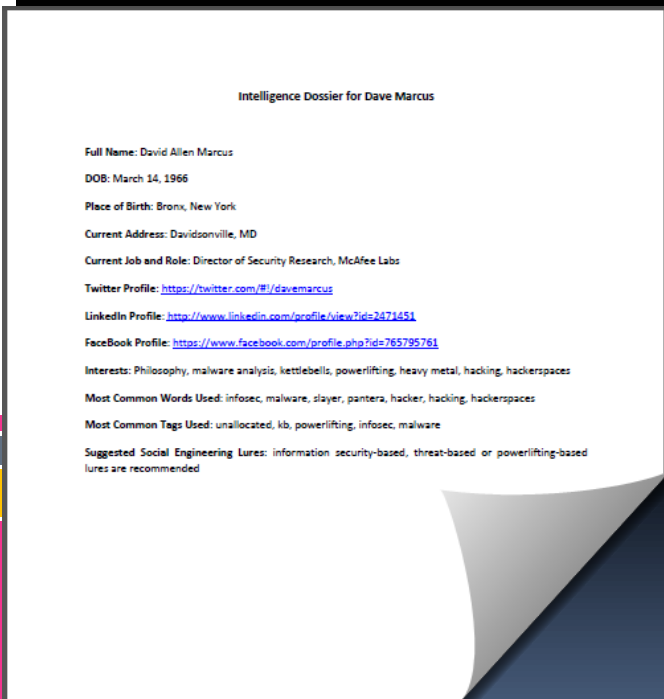
- movie :)
- "happy hour" near:SF
- #haiku
- "listening to"
- love OR hate

What did we learn about Dan?


- OS and Applications
- His Hobbies, Likes, Dislikes and Political Opinions
- His Employment History
- His CURRENT Address and Places He Has Lived
- His CURRENT Phone Number
- His Friends and Contacts

How do we put it into action??

- Build out dossier of intended target based on reconnaissance



- Find and Identify Weaknesses
- Find and Identify Strengths
- Find and Identify Politics
- Identify and Craft Social Engineering Lures
- Own Them



But where can I get a cool
dossier or social
engineering worksheet???

Why at @unallocated of course!

OSINT Dossier and Social Engineering Worksheet

Full Name:

DOB:

Place of Birth:

Current Address:

Education Level and Schools Attended:

Current Job and Role:

Marital Status and Disposition:

Twitter Profile:

- Most Common Tweet Topics
- Most Common Tags Used

LinkedIn Profile:

- Professional Group Affiliations and Memberships

FaceBook Profile:

- Friends, Affiliations and Groups
- Most Common Topics

<http://mcaf.ee/807b6>



Questions??

What can we do?

- Develop “healthy skepticism”
- Get to know your application settings COMPLETELY
- Get to know your devices COMPLETELY
- Get to know your device settings COMPLETELY
- Decide your level of transparency and comfort
- Take action and change behavior
- Tell and show others