Gathering Logical OSINT

Jerod Brennen
CISSP, INFOSEC GEEK

@slandail www.slandail.net

Overview

Company relationships

Public interaction

Technology needs

Logical Reconnaissance

Accumulated information for partners, clients and competitors

According to Verizon, 97% of breaches were linked to a partner

How Strong Is Your Target?

Business Partners, Clients, and Competitors (L1/L2/L3)

Distinguishing Characteristics

Business Partners

Business Clients

Business Competitors

Why is this important?

Social Engineering

An attack vector that relies on the social (human) element to circumvent security controls by deceiving the targets and exploiting their trust

Social Engineering Scenarios

Impersonate a partner

Impersonate a client

Impersonate a competitor

```
site:company_domain.com partners
site:company_domain.com customers
site:company_domain.com clients
company_name competitors
company_name “case study”
```

Search Engine Queries

Usage: Identify logical connections between target organization and external entities

Hoovers Profile (L1, L2)

Hoovers

- http://www.hoovers.com/

Company Information

Industry Analysis

Sales Leads

Hoovers Searches

Search for a Company

Search for a Person

Search for an Industry

Hoovers Subscriptions

$50 USD
per user per month

$87 USD
per user per month

$144 USD
per user per month

Address

Phone Number

Website

Rankings

Competitors

Company Profile

Free Access

Company Report

Industry Reports

Competitive Reports

Technology Report

Paid Access

Hoovers Alternatives

Free

- Google Finance
- Yahoo Finance
- LinkedIn

Paid

- Data.com (Salesforce)
- InsideView
- ZoomInfo

Marketing Information (L1/L2/L3)

Three Areas

Product Line
(L2/L3)

Marketing Vertical
(L1)

Marketing Accounts
(L2/L3)

Product Line (L2/L3)

Products

Services

Support

Market Vertical (L1)

Technology

Service Providers

Data Breaches

Verizon Data Breach Investigation Report

Who was breached?

How were they breached?

How did they respond?

Chronology of Data Breaches

- http://www.privacyrights.org/data-breach

Online database

Restrict searches to similar verticals

Marketing Accounts (L2/L3)

- Facebook
- Twitter
- YouTube
- Pinterest
- Instagram
- Tumblr
- LinkedIn

Important Dates (L1/L2/L3)

Categories

Meetings (L2/L3)

Significant Company Dates (L1/L2/L3)

Significant Company Dates

- Board Meetings
- Holidays
- Anniversaries
- Product/Service Launch
- Fiscal Year

Meetings

Are meeting minutes published?

Are meetings open to the public?

```
company_name “meeting minutes”
site:company_domain.com filetype:pdf meeting minutes
site:company_domain.com calendar
site:company_domain.com events
```

Search Engine Queries

Usage: Locate meeting minutes and significant company dates.

Technology Needs (L1/L2)

Companies Need Two Things

Technology to enable their business

Skilled staff to implement and support that technology

Categories

Job Openings (L1/L2)

RFP, RFQ, Public Bid Information (L1/L2)

Job Search Sites

Indeed

Monster

CareerBuilder

ComputerJobs

Dice

Technical Support

System Administrator

Database Administrator

Application Developer

IT Architect

Security Analyst

Security Engineer

Job Search Terms

Public Bid Information

Request for Proposal

Request for Quote

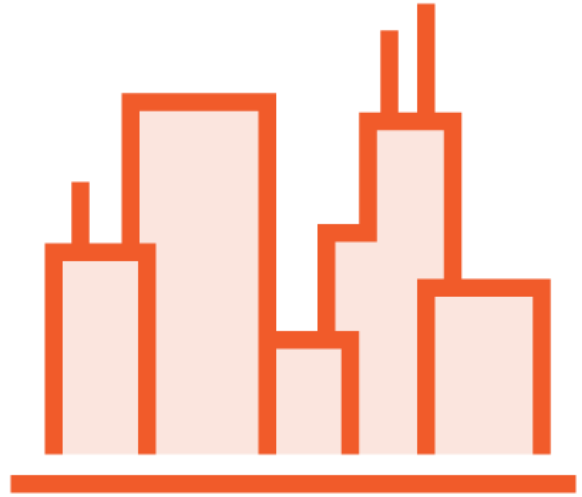
Public Disclosure (L1/L2/L3)

Categories

- Charity affiliations (L1/L2/L3)
- Political donations (L2/L3)
- Court records (L2/L3)
- Professional licenses or registries (L2/L3)

Charity Affiliations

National/International



Local/Regional

Popular Charities

National/International

Red Cross

Doctors Without Borders

World Wildlife Fund

UNICEF

World Vision

Local/Regional

Service organizations

Homeless shelters

Disease research

Conservation and preservation

```
county_name “court records”
company_name filetype:pdf “v.” “syllabus”
company_name filetype:pdf “v.” “plaintiff”
company_name filetype:pdf “v.” “defendant”
company_name filetype:pdf “v.” “case no.”
```

Search Engine Queries

Usage: Locate court records

Political Donations (USA)

Federal Election Commission

Federal Lobbying Disclosure Act (LDA) Compliance

OpenSecrets

Professional Licenses or Registries

Industry/Vertical vs. Website

Licensure or Registration Organizations

Requirements

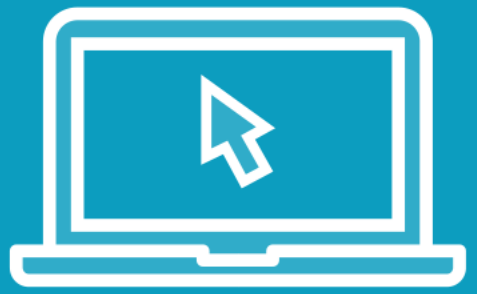
market_vertical professional license

market_vertical company registry

Search Engine Queries

Usage: Locate professional licenses or industry registries

Demo



Bug bounty program: Spotify

- https://bugcrowd.com/spotify

Summary

Partners, clients, competitors

Hoovers

Marketing information

Important dates

Technology needs

Public disclosure

On to the next module: Constructing an Org Chart