

# RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HUM-R04

## COMPROMISING FORTUNE 500 BUSINESSES WITHOUT HACKING A THING!

### Rachel Tobac

CEO, SocialProof Security  
UX Research, Course Hero  
@RachelTobac / @socialproofsec

### Joe Gray

Senior Security Architect, IBM  
@C\_3PJoe / @advpersistsec /  
@hackingglass

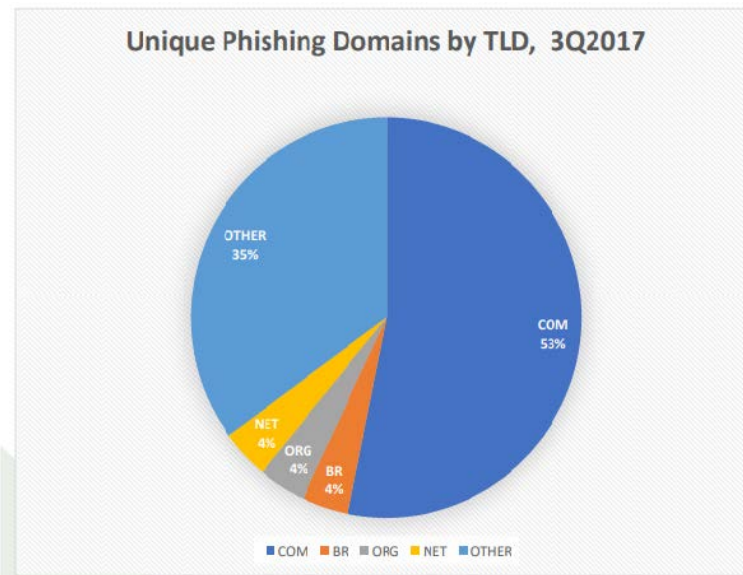
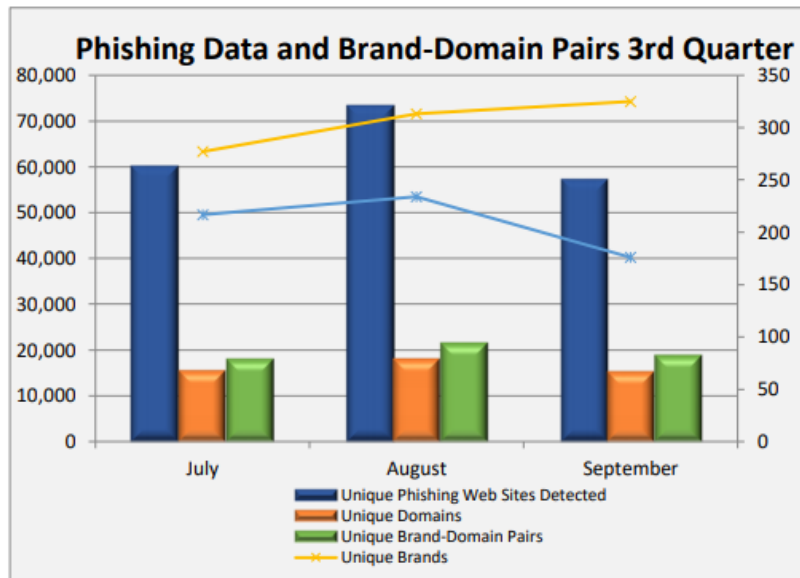


#RSAC

# The Cold Hard Facts



# Phishing Statistics



Source: APWG 3Q2017 Report



# Statistic Highlights



## Statistical Highlights for 3<sup>rd</sup> Quarter 2017

|  | July   | August | September |
|--|--------|--------|-----------|
| Number of unique phishing websites detected  | 60,232 | 73,393 | 57,317    |
| Number of unique phishing e-mail reports (campaigns) received by APWG from consumers | 99,024 | 99,172 | 98,012    |
| Number of brands targeted by phishing campaigns                                      | 277    | 313    | 325       |

Source: APWG 3Q2017 Report

# About Rachel @RachelTobac



# About Joe



## DERBYCON VII (2017) CLOSING CEREMONY

Chris Hadnagy presenting me with the Trophy



# Apply! What will you learn today?



- OSINT concepts and how they lead to social engineering (SE) attacks
- Common social engineering attack methods
- How we won SECTFs
- Examples of what social engineering sounds like
- How to get your organization prepared for SE





## HOW WE DO OPEN SOURCE INTELLIGENCE

OSINT against the business and its users



# What is OSINT?



#RSAC

## Publicly available material:

- The Internet
- Traditional mass media
- Specialized journals, conference proceedings, and think tank studies
- Photos
- Geospatial information
- Social media



# What OSINT info do SEs target?



- VPN
- ESSID name
- Make and model of computer
- OS info + service pack/version
- PDF reader
- Browser and version
- Mail client
- Disk encryption
- Any/all software/versions

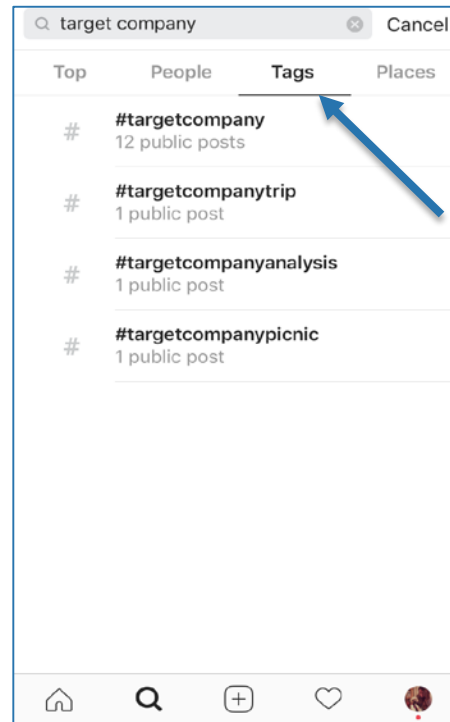
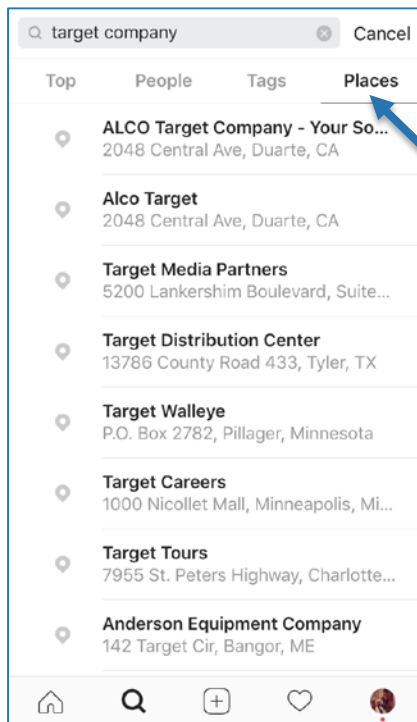


# How I use social media for most OSINT





# Instagram OSINT Example



# Facebook OSINT Example



**Search is Back!**  
Find people and events on Facebook  
Search by location, job, and relationships!

FIND PEOPLE | EVENTS | POSTS & SHARES | PHOTOS

Search for:

Gender:

Interested in:

Relationship status:

Current location:

Interest:

Current company:

Current school:

Job title:

Language spoken:

Major:

Born:  :

Name:

[Created by Michael Morgenstern]

**Search is Back!**  
Find people and events on Facebook  
Search by location, job, and relationships!

FIND PEOPLE | EVENTS | POSTS & SHARES | PHOTOS

Text in post:

*Note: If you want to search by text, choose Any posts instead of Friends or Friends of Friends.*

[Created by Michael Morgenstern]



# Gaining Initial Information



RSA Security LLC: Private Com... X

Bloomberg L.P. (US) https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=34160 133% Search

February 12, 2018 11:54 PM ET

## Software

### Company Overview of RSA Security LLC

**Snapshot** **People**

#### Company Overview

RSA Security LLC provides intelligence-driven security solutions primarily in the United States. The company's solutions help organizations protect their information and manage the identities of the people and applications accessing and exchanging that information. It offers technology solutions, including authentication and credential management, access management, identity administration, and data protection. In addition, the company provides business solutions, including regulatory compliance, password management, consumer identity protection, portal and partner integration, mobile workforce security, and credit/debit card information protection. It serves banking, insurance, technology, ...

**Detailed Description**

174 Middlesex Turnpike  
Bedford, MA 01730  
United States

Phone: 781-515-5000  
Fax: 781-515-5010  
[www.emc.com/domains/rsa/index.htm](http://www.emc.com/domains/rsa/index.htm)

Founded in **1982**  
**1,282** Employees

#### Key Executives For RSA Security LLC

**Mr. Arthur W. Coviello Jr.**  
Former Executive Chairman  
Age: 64

**Mr. Mark Quigley**  
Senior Vice President and Chief Operating Officer

**Ms. Niloofer Razi Howe**  
Chief Strategy Officer and Senior Vice President  
Age: 48

**Mr. Doug Howard**  
Vice President of Global Services

**Mr. Jonathan Gill**  
Vice President of Europe, Middle-East & Africa

Compensation as of Fiscal Year 2017.

#### S&P Global Market Intelligence

The information and data displayed in this profile are created and managed by S&P Global Market Intelligence, a division of S&P Global. Bloomberg.com does not create or control the content. For inquiries, please contact S&P Global Market Intelligence directly by clicking [here](#).

#### Stock Quotes

Market data is delayed at least 15 minutes.

Stock, Fund, or ETF  [Company Lookup](#)

#### Most Searched Private Companies

| Company Name                                   | Geographic Region |
|--|-------------------|
| Lawyers Committee for Civil Rights Under Law   | United States     |
| The Advertising Council, Inc.                  | United States     |
| Tax Management Inc                             | United States     |
| NYC2012, Inc.                                  | United States     |
| John F. Kennedy Center For The Performing Arts | United States     |

#### Sponsored Financial Commentaries

#### More From The Financial Web

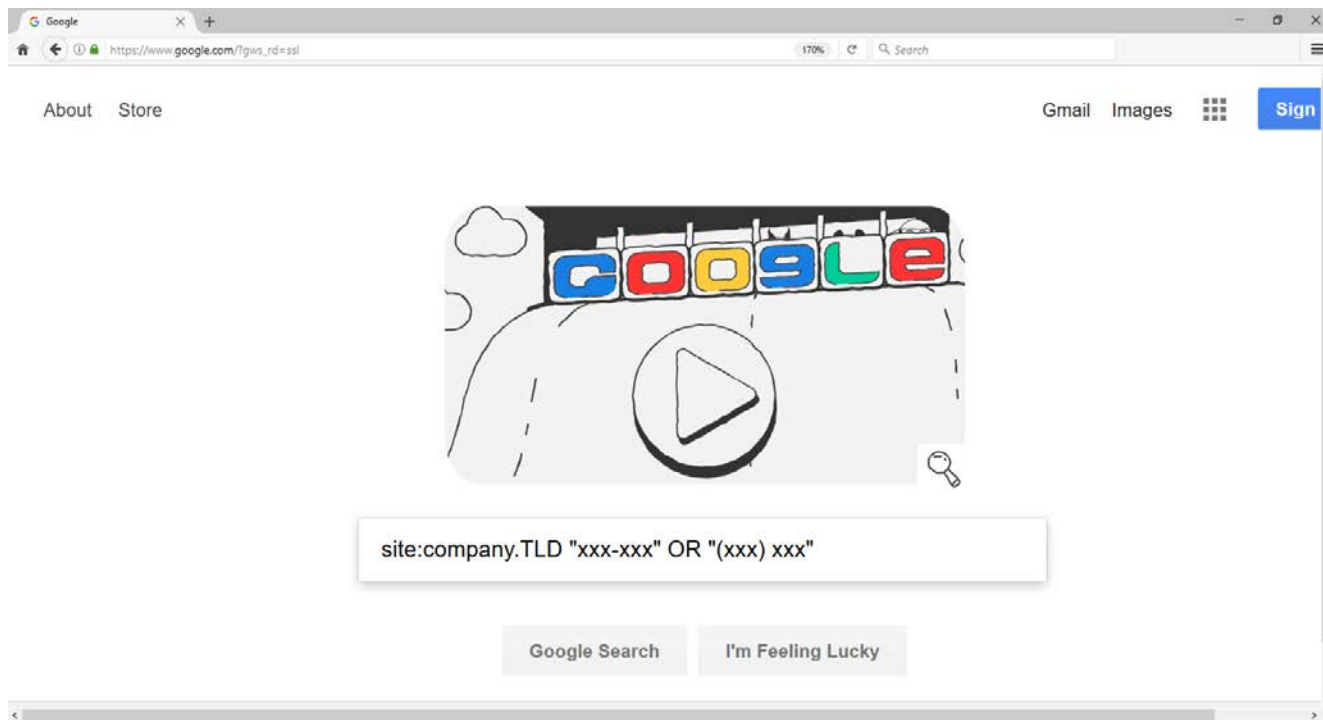




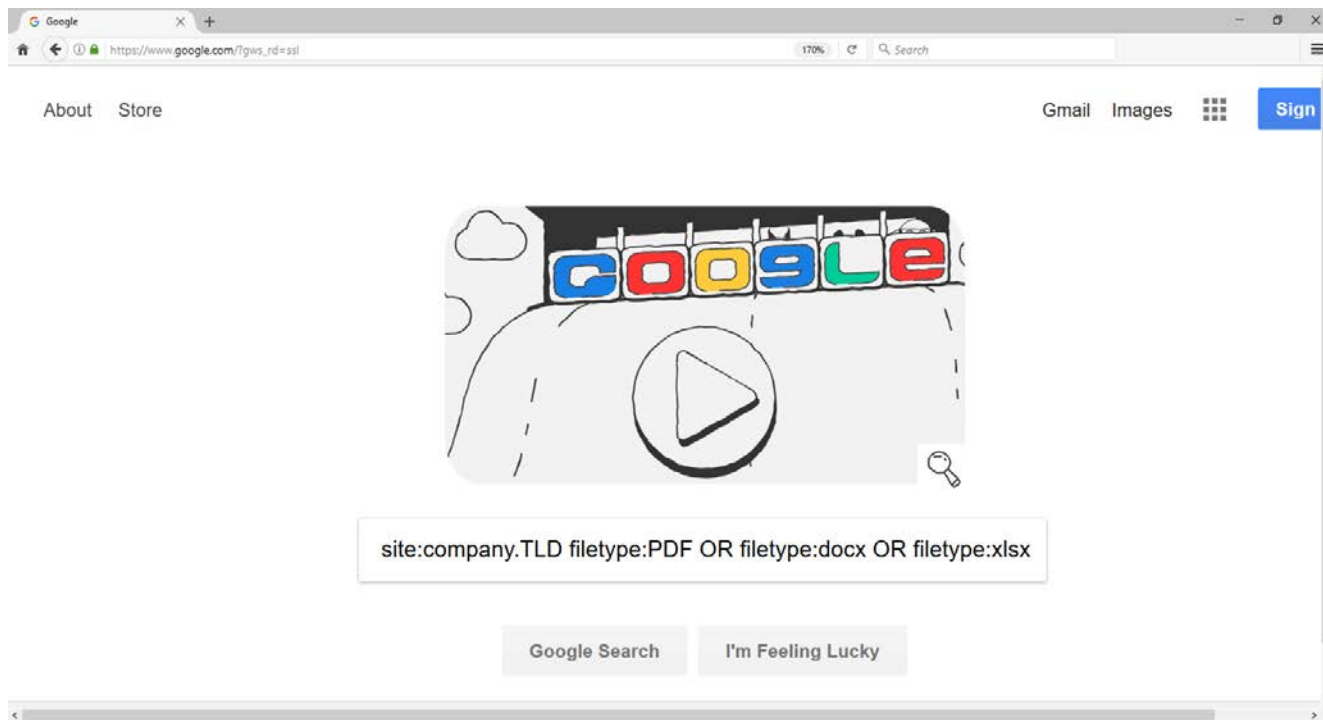
# OSINT for Phone Numbers



- Block your number and sweep the organization
- Call outside hours to get names from voicemail
- If you find the directory, search for common last names



# Google-Fu Next Step





# Finding Info on People



- Build a repository of people
- Enumerate the people

# Finding Info on People Continued



- See what user names they use
- Look for goldmines
- Use this data to build dossiers and leverage it to build rapport

# About the domains



- Enumerate information about domains
  - Subdomains
  - MX records
  - SPF
  - Technologies used
    - Remote.target.tld
    - VPN.target.tld

# We Take a Tour





# How do SEs use these data points later?





## SOCIAL ENGINEERING



**Any act that convinces someone to do something that may or may not be in their best interest.**

@RachelTobac

# Picking Targets



- I wish the phone numbers I can find
- 3rd party vendors posting and tagging you
- You help people? You're getting a call
- You posted on social media about your company



# Picking Pretexts





# Why does SE work on people so well?

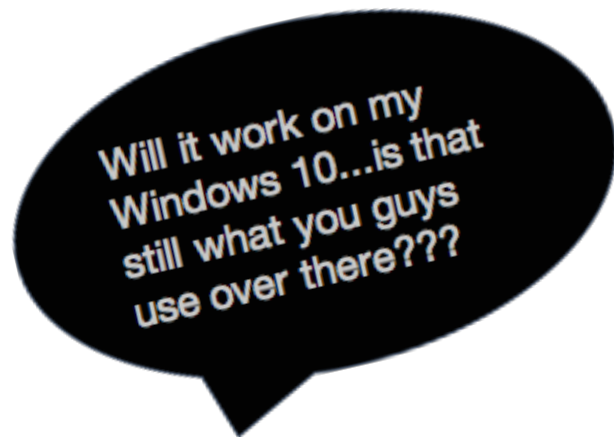


- **Cialdini's 6 Principles of Persuasion:**

- Reciprocity
- Commitment & Consistency
- Social Proof
- Liking
- Authority
- Scarcity



# DEFCON SE calls



@RachelTobac  
RSAConference2018



## Props

- Office Noises
- Uniforms
- Toolboxes
- Ladders
- Donuts and/or Coffee
- Badges

**RSA**Conference2018

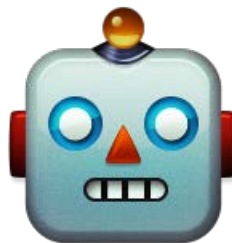


#RSAC

## **BRINGING IT ALL TOGETHER: NEXT STEPS**



# Emoji Takeaways



# Training should be timely



 2014 · 

All day   
Information Security Awareness Training.....  
ALL DAY!!!!

 Share

 1

 Sounds thrilling!  
2014 at 3:12pm

 That's good for ya!  
2014 at 3:38pm

# Tips for Training



- Do more than the annual training for compliance purposes
- Employ role based training
- Integrate into Incident Response Plan
- Use automated solutions or external contractors to attempt attacks
- Ensure social engineering (specifically phishing, pretexting, and vishing) are included in your penetration tests

# Applying what you've learned



- Next week you should:
  - OSINT survey on your company
  - talk with management about SE
  - talk with IR team for integration
- In the first three months following this presentation you should:
  - quarterly training scheduled in a shorter format
  - baseline phishing simulation
- Within six months you should:
  - adapt training to current trends and testing results
  - have a second training session
  - OSINT survey and Social Engineering pentest



# Resources



- <https://github.com/jocephus/RSAC> Resources/

RSA Conference 2018



#RSAC

## QUESTIONS?



@racheltozac  
@C\_3PJoe

