RSAConference2018
San Francisco | April 16 – 20 | Moscone Center


SESSION ID: HT-W04

# IDENTITY THEFT THROUGH OSINT

**Zee Abdelnabi**

Manager/Security researcher
Big 4
Infosec_17

I am very happy with her!

YOUR CHILD CHOOSES THESE ACTIVITIES work skills

| JANUARY | JUNE |
| --- | --- |
| | Math |
| | Computer |

ORE 6-17-91

PINK COPY - Parent (January)

OPY - Parent (June)


HACK THE PLANET!


INFO SEC
HACKING????
Zee meets FBI
NEIGHBOR··
I CAN'T WAIT TO HACK THE WORLD


LIVE

# Attackers perspective



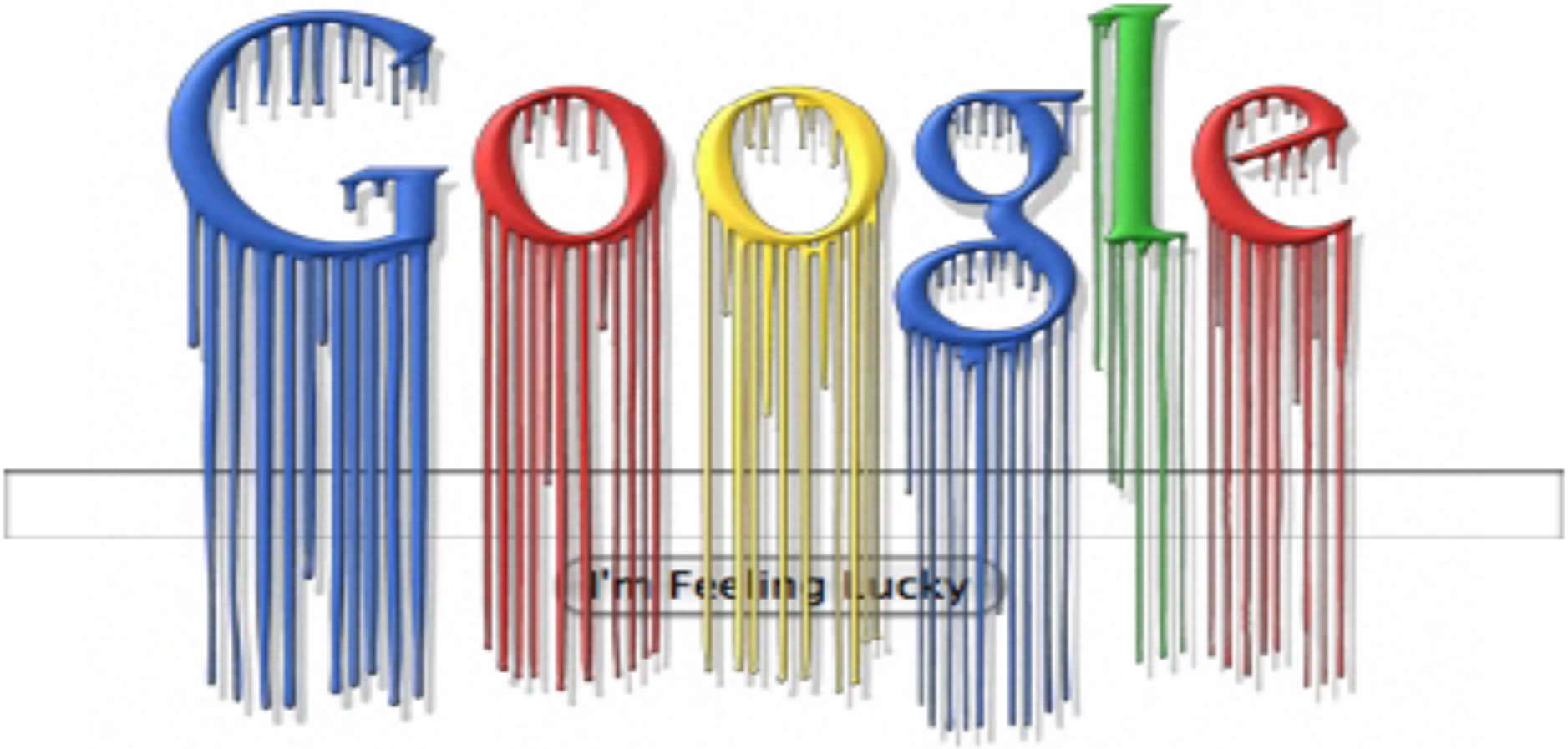
- What does the attacker do and what does the victim go through?
- How do we detect fraud? In most regards you cant until its too late!

# OSINT



- Open source intel from public resources
- Image intelligence
- Search engines, blogs, meta data from pics, media, cons, executables, docs, tv
- Reduce amount of noise getting the information
- Help maximum your attack

# HACKING WITH



# The basics



- “client in quote” “payroll” “janitor” “policies” “portal”
- Filetype pdf “itt tech” “employee handbook”

please visit ntitle i-catcher console

All Shopping Videos Images News More Settings Tools

About 61,000 results (0.41 seconds)

Including results for please visit ***intitle*** i-catcher console
Search only for please visit ntitle i-catcher console

"please visit" intitle:"i-Catcher Console" Copyright "iCode Systems"
https://www.exploit-db.com/ghdb/640/
Nov 3, 2004 - Google Dork Description: "**please visit**" **intitle**:"**i-Catcher Console**" Copyright "iCode Systems". Google Search: "please visit" intitle:"i-Catcher ...

i-Catcher Console - Live view
72.36.1.86.static.actaccess.net/
Java was not detected in your browser. To continue using the web view, **please** select "JavaScript" on the left. To improve the performance of the **i-Catcher** Web ...

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Reverse image search

- Images.google.com
- Tineye.com

# Fraud and hacking



- Social media is an amazing tool for harvesting information
- --how many people befriend complete strangers
- --acquaintances?
- --Good friends?

# Common info people post

- Current locations
- Employer
- Email
- Home address
- Phone number

# Why do you use social media?



- Job hunting
- Activism
- Self promotion
- Education
- News
- Sports
- community

# Hacker

- Building layout
- On-guards
- Security systems in place
- Vendors
- Dumpsters
- Janitorial services
- Network diagrams
- Internal lingo
- Photos
- Badges

# Password cracking



- DOB
- Hospital of birth
- List of schools
- Previous addresses
- Middle name
- Place of birth
- Pet’s name
- Hobbies
- Relatives
- Mothers maiden name

# Investigator

- Employer
- Favorite Locations
- Photos
- Associates
- Websites visited
- Blogs, forums,
- Email addresses
- Home addressed
- Current location
- Past internet activity
- Evidence of crime
- Aliases

# Social Engineer



- Customer, tech repair
- Auditor
- Phishing is free
- We like to believe convenient lie not truth

# Attackers perspective



- Who is that person
- What does he do
- What does he like
- How do they go about their days
- Public Social Media

# Attackers Perspective



- What's the end goal?
- Identity theft getting more difficult people getting familiar with tactics.
- I want to know the smallest details, how you think.

# How did I pick my target

- Random guy
- Blog at random guy.com
- http://jccsst-random.blogspot.com/p/who-am-i.html

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

### Shipping Clerk
Lippert Components, Inc.
October 2014 – Present (2 years 5 months) | Elkhart, Indiana Area

### Materials Handler
Tenneco
March 2014 – September 2014 (7 months)

### Operator
AACOA, Inc
October 1999 – March 2014 (14 years 6 months)

## Volunteer Experience & Causes

### Activites volunteer
Riverview Nursing Home
June 1985 – September 1988 (3 years 4 months) | Health

## Skills

Automotive · Continuous Improvement · Lean Manufacturing · Kaizen · 5S · Manufacturing · Forklift Operator · Warehousing · Logistics · Materials Management · Six Sigma · Vehicles · Supply Chain Management · Inventory Control · Anodizing

See 12+

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

Private research shown during talk

# Private research shown during talk

Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# What next?

- Know his activities; what he likes doing
- Member of groups
- Can I spoof his email so I can send him an attachment if I know his email
- Email him relevant information and with a malicious attachment that doesn't do much and its not suspicious

# Attack Surface



- Using what they know and what they like is standard SE getting foothold through their company.
- What if they are working on their work computer… or BYOD… wait and own their corporate network and gives you a foothold based off identity theft.
- Working from home if using VPN opens up a large attack surface.
- Waiting to see if they type in bank creds and things like that.

Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Private research shown during talk

# Internally

- Computers infected on a work domain are doing things like packet inspection to see if a social security is going over the network (dlp) and why?
- Are we getting lots of spam targeting certain individuals?

# Private research shown during talk

# Use of independent system or BYOD allows for greater foothold of fraud…

# Actionable Intel

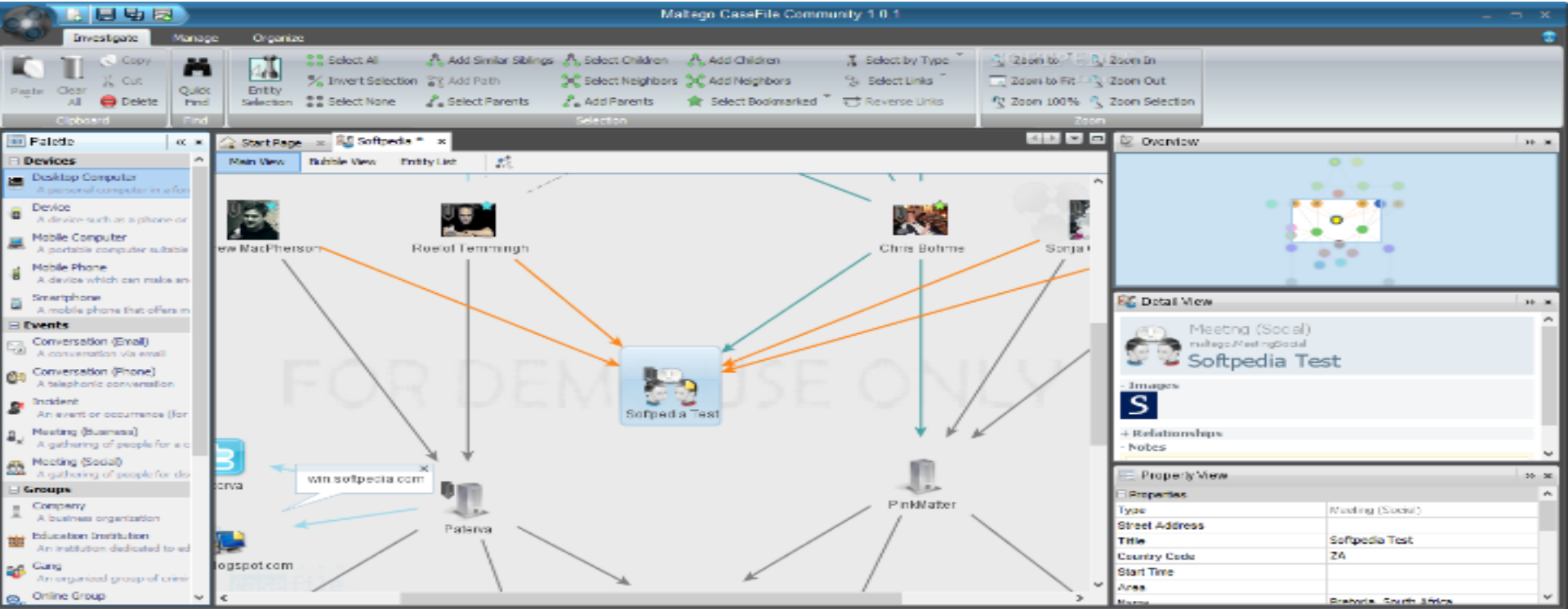


- How your getting his data and what you are going to do with it?
- How much info did he expose on internet?
- Sharing info at a very high rate can be used against them in an attack?

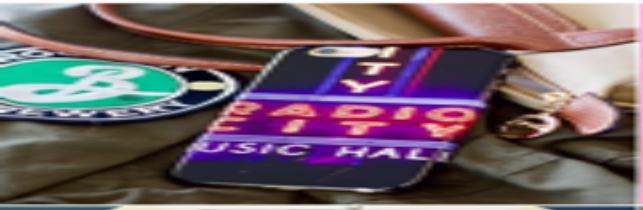
# CaseFile: build a web of that person

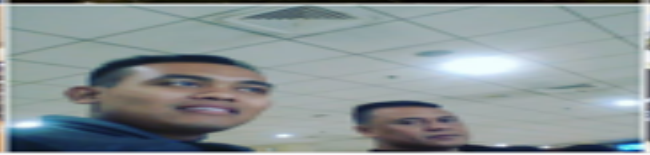


Quality and quantity of data and how you represent that data…




$99/1個
$160/2個


RADIO
CITY
MUSIC HALL




RADIO
CITY

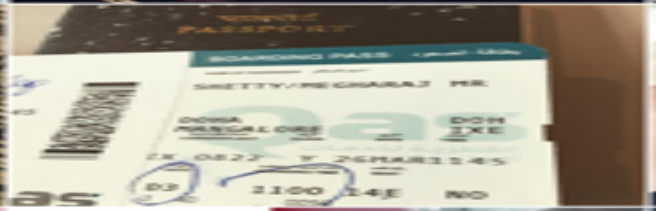
# #boardingpass

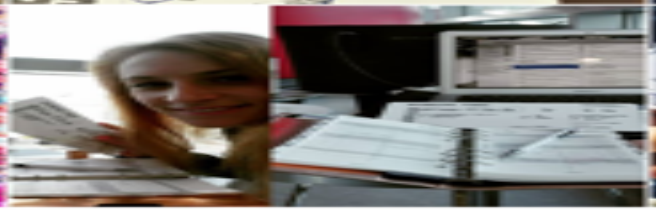
Related: #boardingpasses #boardingtime #departure #busine

## TOP POSTS



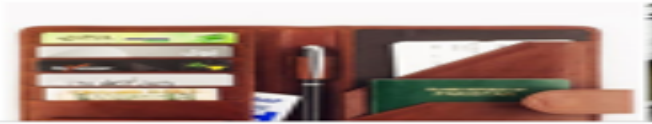





## MOST RECENT

85,068 posts




thewellnessvoyager Follow


11 likes

thewellnessvoyager Hello Dubai ✈✈✈✈✈✈ #timetotravel #lifeisanexperience #lifeisonebigadventure #Dubai #travels #traveller #experiences #explore #timetoenjoy... more

2 HOURS AGO

# Bar Code Cracking



- First name, last name
- Frequent flyer #

T-Mobile Wi-Fi 12:42 PM

TOP POSTS

# #bankcard

trngduy Follow


109 likes

trngduy 은행카드 😍😍 자산 😂😂
#assets
#bankcard
#ATM

MOST RECENT

# #bankcard

linda.bzh Follow ...


19 likes

**linda.bzh** Instageek acte 1 : clé USB dans une carte bancaire. Pratique pour la ranger 😉 USB key in a bank card 💳 .Convenient to store. #instageek #instageeks #usb #bankcard #geeklife #geek🤓 #geekette

MARCH 14 · SEE TRANSLATION

monsterweb.cz Follow ...

# Verify

- Don’t accept friend invites from people you don’t know even if they have 202 mutual
- Check the age of social media profiles
- Reverse image search the photo

Adriana

# Who is



- https://www.familytreenow.com/optout
- https://www.instantcheckmate.com/optout/
- http://www.peekyou.com/about/contact/optout/
- http://www.spokeo.com/opt_out/new
- https://www.beenverified.com/f/optout/search
- https://secure.whitepages.com/me/suppressions
- http://www.peoplefinders.com/manage/
- https://www.peoplesmart.com/optout-go
- https://www.usa-people-search.com/manage/
- https://radaris.com/
- https://www.peoplelooker.com/f/optout/search

# “Apply” Slide



- Next week you should:
  - Have a clear visibility into your social media attack surface
- First three months following this presentation you should:
  - Limited and removed all public information and pictures.
- Within six months you should of:
  - Educated your family and friends on identity theft and how hackers are stealing their identities.