OSINT101:
From a name to a Dossier

Or, How we Doxxed[1] an Executive and kept our jobs!

Who are we?

IBM Security

- IBM X-Force Ethical Hacking Team
  - IBM Security's internal pen-test team

Presenting
- Warren Moynihan
- Dmitriy Beryoza
- Chris Shepherd

Others
- Rodney Ryan
- John Zuccato
- Jonathan Fitz-Gerald

Obligatory -covering Slide

Opinions are our own and not of IBM!

Agenda

- Overview of what we did and why
- The meat and potatoes of OSINT
  - We’ll walk through turning the simple information we got into a full on dossier
- Applying the information
- What did we learn?

Why did we do it?

- We wanted to apply threat modeling techniques to an individual
- Had research time over the holidays
- Executives are tempting targets
  - Even clipart knows this:

Limitations

- Passive-only recon
  - Our target, “Duke Johnson”, knew about this
- Duke works in infosec
- Duke lives in New Jersey
  - We’re all in Ottawa
- Our funding was two stale doughnuts we found in the bottom of a drawer
- Only had one week

The Cake is a Lie

- All of the information we're about to cover is obfuscated to protect the privacy of the real person
- Names, locations, hobbies, dates of birth, etc. are all fictitious
- Represents the information or types of information we discovered

How did we do it?

- Started from a name - “Duke Johnson” who works for IBM
  - We knew very little about Duke but we did have a rough idea of where he lived
  - Knowing even vaguely where he lived didn’t matter because we found Duke’s LinkedIn profile quickly

LinkedIn

- LinkedIn provided a bunch of useful info:
  - Duke's e-mail address
  - City and State where Duke lives
  - Prior employers
  - Education + Schools
  - Duke's employee number for prior employer
    - Plus a photo of his old work badge!
  - List of business colleagues/relationships
  - Patents filed by Duke and a former colleague
    - Gave us Duke's full name including middle initial

The e-mail address is the lynchpin of recon

- Searching via e-mail yielded several accounts:
  - Standard social media
    - Facebook / YouTube / Google+
  - Photobucket
    - Also led to another e-mail address
  - Dog showing forums

Other e-mail results

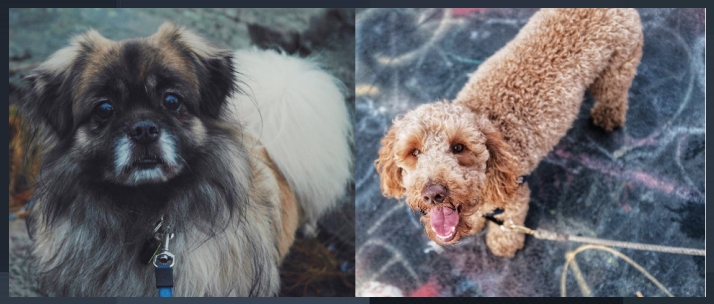
- We also discovered several aliases he uses online:
  - DJ11 (dog showing)
  - Nukem
  - Nik9door44
  - Djjohnson1
- With usernames you can easily find sites with the same account name via services like NameChk, KnowEm, ThatsThem, etc.
  - Recon-ng, spiderfoot, etc. also very useful tools
- **OSINT Framework is a great starting point**

Aunt Betsy Will Tell On You

- Found Duke’s entire family courtesy of his full proper name and a helpful relative
  - Team member had a paid Ancestry.com account
  - Just added “Duke Thomas Johnson” in NJ
  - Two days later an e-mail arrives with a “this might be your family tree” suggestion
  - Said relative had filled everything out, including pictures of parents and obituaries
- Lesson: Whatever you decide to secure, a person will probably undo it for you
- Some jurisdictions have privacy laws around this
  - You can frequently get around these by visiting in person and paying a fee

Putting a face to the name

- Profile picture on several forums
- Able to find new accounts via reverse image search
- Also found family and pets



Social Media: Working the Photomines

- Pictures are worth at least a thousand words
  - 5 pictures = Photo essay?
- Photos posted to Facebook, Instagram and Photobucket yielded a lot of information:
  - Devices (laptops, phones, etc.)
  - License plates for vehicles
  - Confirmation of layout of the house
  - Details about the layout of the property, including photos of locks
  - Information about Duke's particular favourite music and bands
  - Companies that Duke was a customer of
  - Friends' pictures of Duke revealing identifying marks on the body (think Tattoos, moles, etc.)
- This info came from normal "sharing your life" posts
  - Some of them very old – **nobody ever cleans up**!

Haveibeenpwned? You mean Haveubeenpwned?

- Anyone can look up where any e-mail address’ data has been leaked via HIBP
- We were able to verify his data was present in several dumps
  - Narrows down which dumps will be interesting to us
- Notable for us: Marketing dumps

A Note on Marketing Dumps

- Why are these valuable?
  - With enough data points we can correlate an “anonymised” record with a real person
  - If you live in Springfield, have three children, work for a utility, and drive a Plymouth Junkarola, you are really likely to be Homer Simpson
  - Tying our research into this we could then find out other things about our target based on the marketing profile
- Per HaveIBeenPwned, there have been to date at least 150 million unique records leaked from marketing sources

Street View

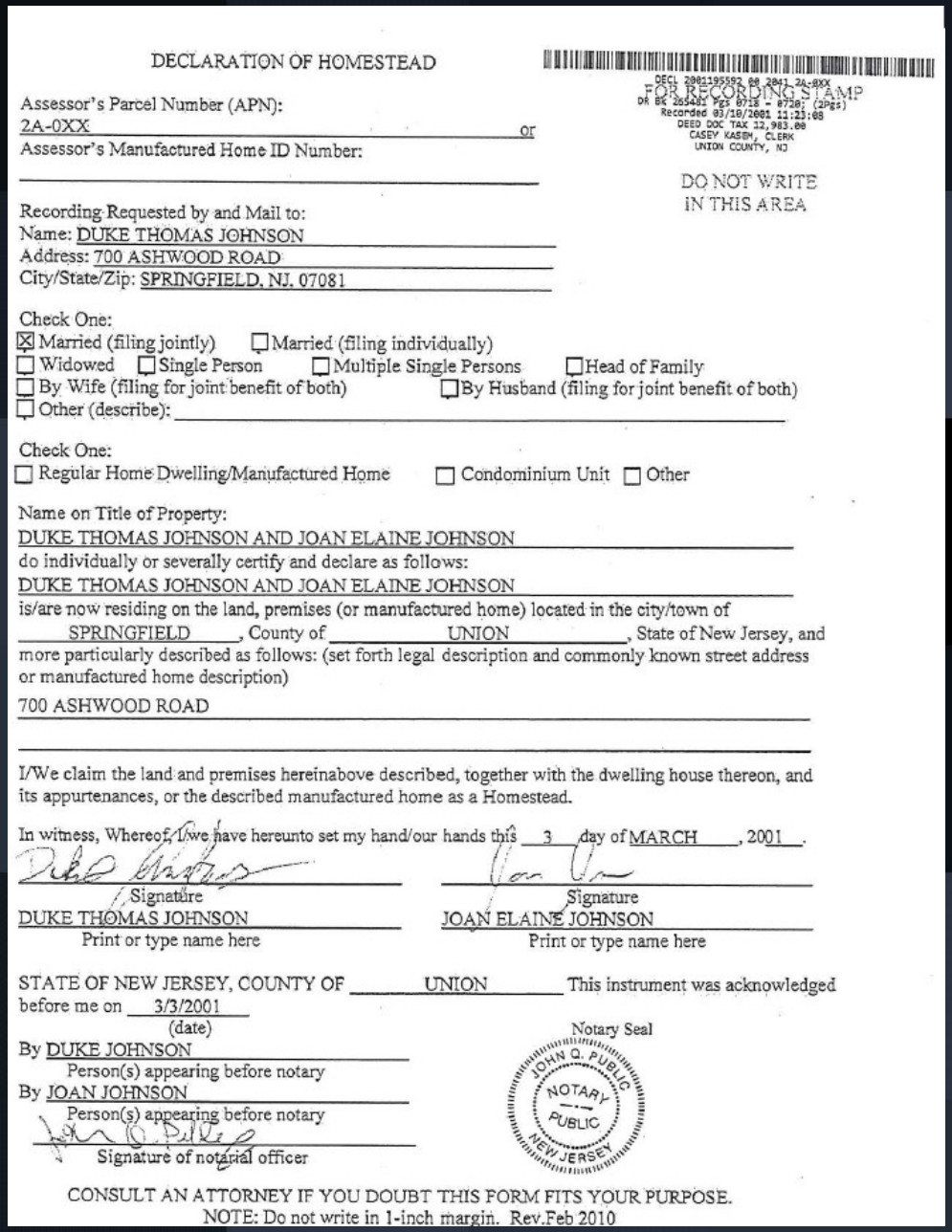
- Duke having some HVAC work done while street view was visiting
- Excellent for further social engineering attacks

Deep Web Research

- Gov’t records offices are goldmines and are often not indexed by search engines
  - Found court cases for relatives
  - Found registered vehicle sales for Duke’s current and previous vehicles
  - For his home:
    - Deed and mortgage papers with signatures
    - Floor plan
    - Land parcel numbers, Aerial photos

Signatures

- This public document shows both Duke and his wife Joan's full legal names as well as their signatures
- Helps with identity theft and similar follow-on attacks



DECLARATION OF HOMESTEAD

DECL 2001195592 08 2041 2A-0XX
FOR RECORDING STAMP
DR BK 265481 Pgs 0718 - 0720; (2Pgs)
Recorded 03/10/2001 11:23:08
DEED DOC TAX 12,963.00
CASEY KASEM, CLERK
UNION COUNTY, NJ

Assessor's Parcel Number (APN):
2A-0XX or
Assessor's Manufactured Home ID Number:

DO NOT WRITE IN THIS AREA

Recording Requested by and Mail to:
Name: DUKE THOMAS JOHNSON
Address: 700 ASHWOOD ROAD
City/State/Zip: SPRINGFIELD, NJ. 07081

Check One:
☒ Married (filing jointly) ☐ Married (filing individually)
☐ Widowed ☐ Single Person ☐ Multiple Single Persons ☐ Head of Family
☐ By Wife (filing for joint benefit of both) ☐ By Husband (filing for joint benefit of both)
☐ Other (describe):

Check One:
☐ Regular Home Dwelling/Manufactured Home ☐ Condominium Unit ☐ Other

Name on Title of Property:
DUKE THOMAS JOHNSON AND JOAN ELAINE JOHNSON
do individually or severally certify and declare as follows:
DUKE THOMAS JOHNSON AND JOAN ELAINE JOHNSON
is/are now residing on the land, premises (or manufactured home) located in the city/town of SPRINGFIELD, County of UNION, State of New Jersey, and more particularly described as follows: (set forth legal description and commonly known street address or manufactured home description)
700 ASHWOOD ROAD

I/We claim the land and premises hereinabove described, together with the dwelling house thereon, and its appurtenances, or the described manufactured home as a Homestead.

In witness, Whereof, I/we have hereunto set my hand/our hands this 3 day of MARCH, 2001.

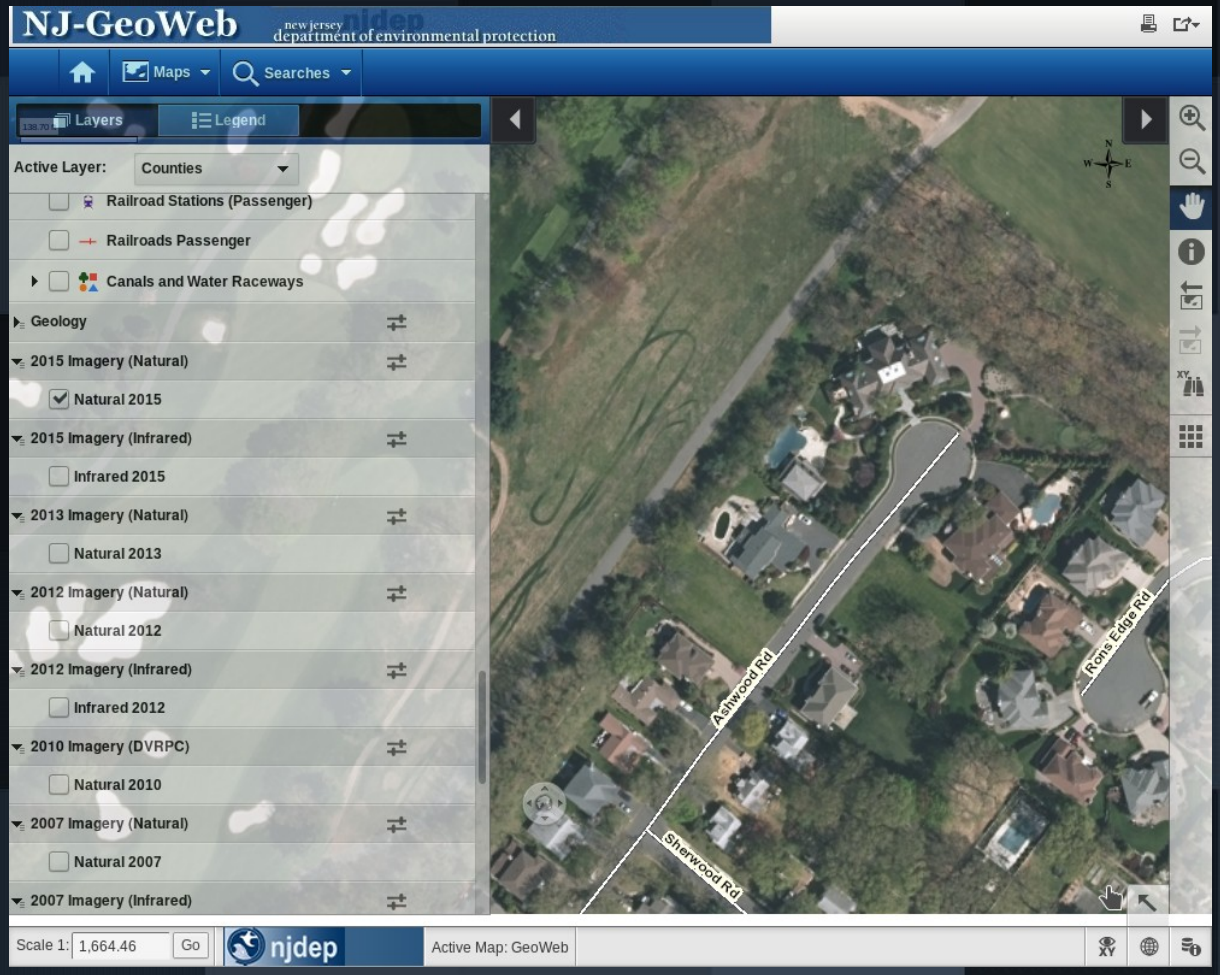
Signature — DUKE THOMAS JOHNSON (Print or type name here)
Signature — JOAN ELAINE JOHNSON (Print or type name here)

STATE OF NEW JERSEY, COUNTY OF UNION This instrument was acknowledged before me on 3/3/2001 (date)
By DUKE JOHNSON Person(s) appearing before notary
By JOAN JOHNSON Person(s) appearing before notary
Signature of notarial officer

Notary Seal
JOHN Q. PUBLIC NOTARY PUBLIC NEW JERSEY

CONSULT AN ATTORNEY IF YOU DOUBT THIS FORM FITS YOUR PURPOSE.
NOTE: Do not write in 1-inch margin. Rev.Feb 2010

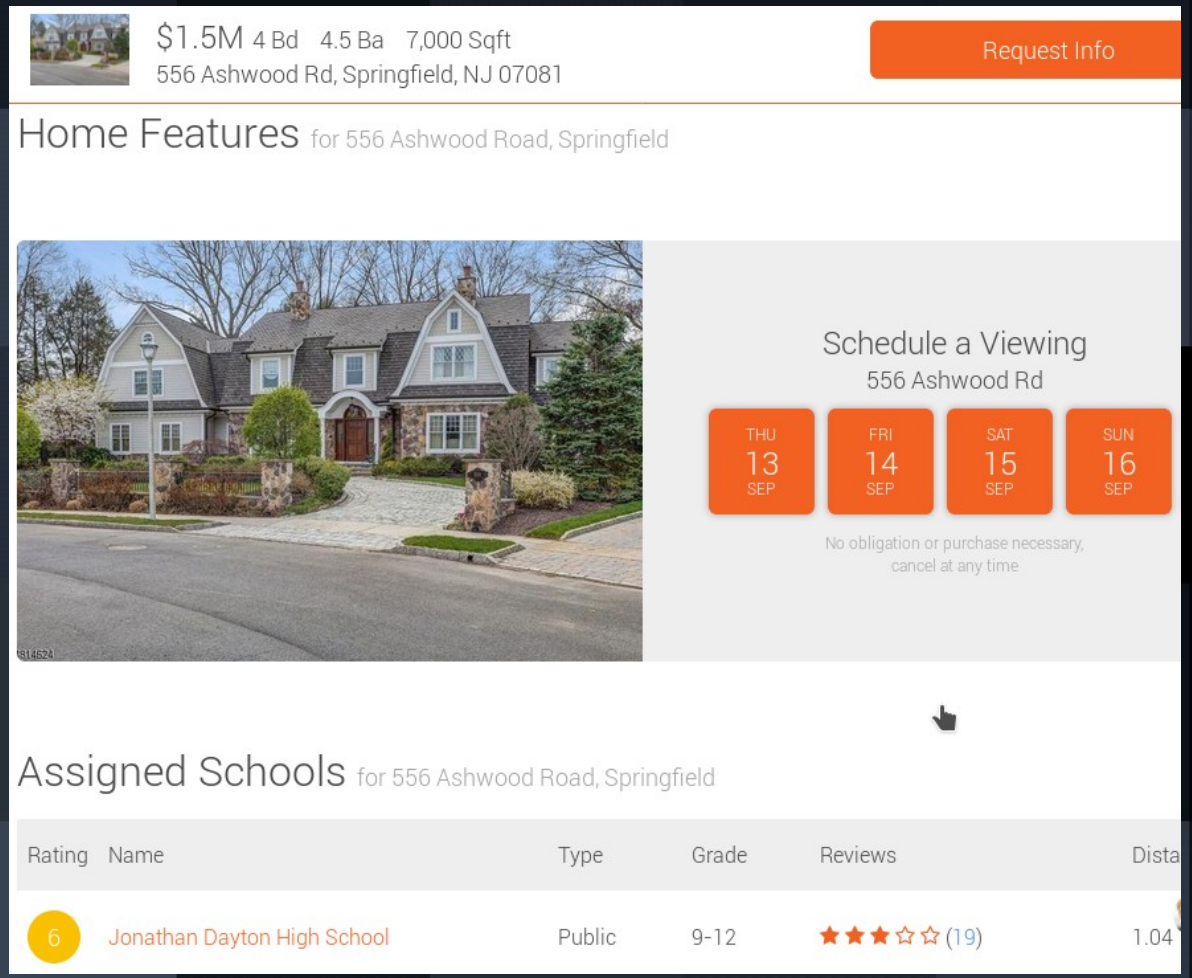
Aerial Photos



- Tells us property layout
- By comparing different years' photos, figured out what time-frame his pool was built
  - This can help with social engineering attacks

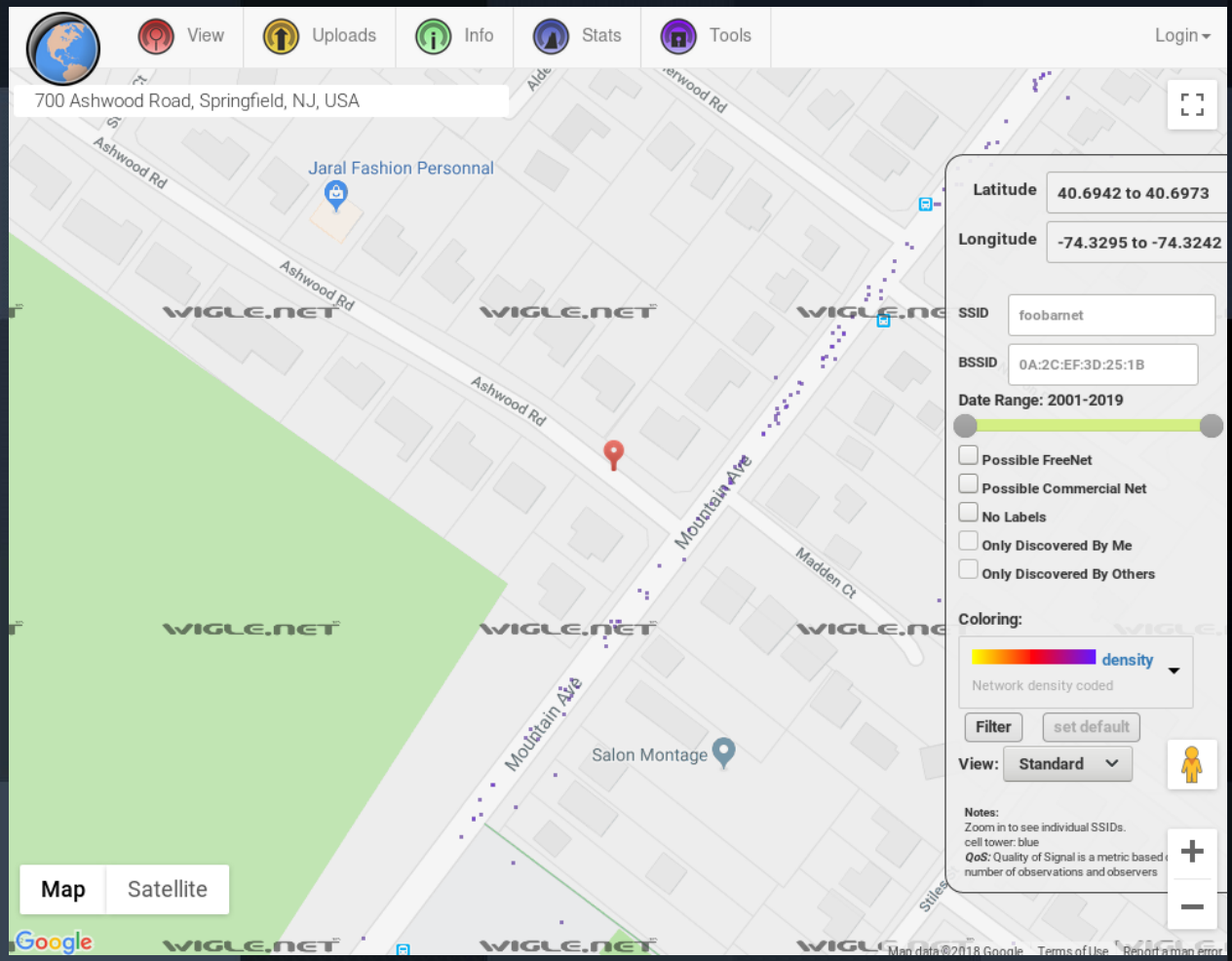
Near Duke's Home

- Nearby homes for sale offer up information about nearby services, schools, etc.
- Also sheds light on property values
- Aids in-person recon
  - Solid excuse to be poking around the area



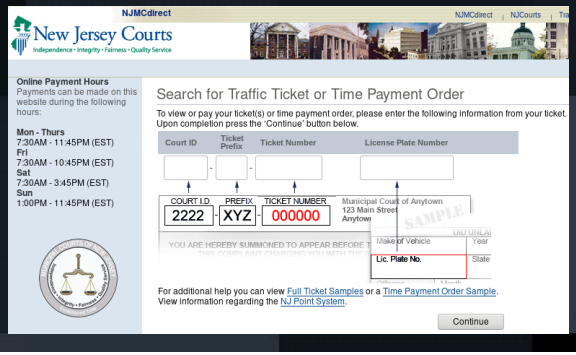
Wireless

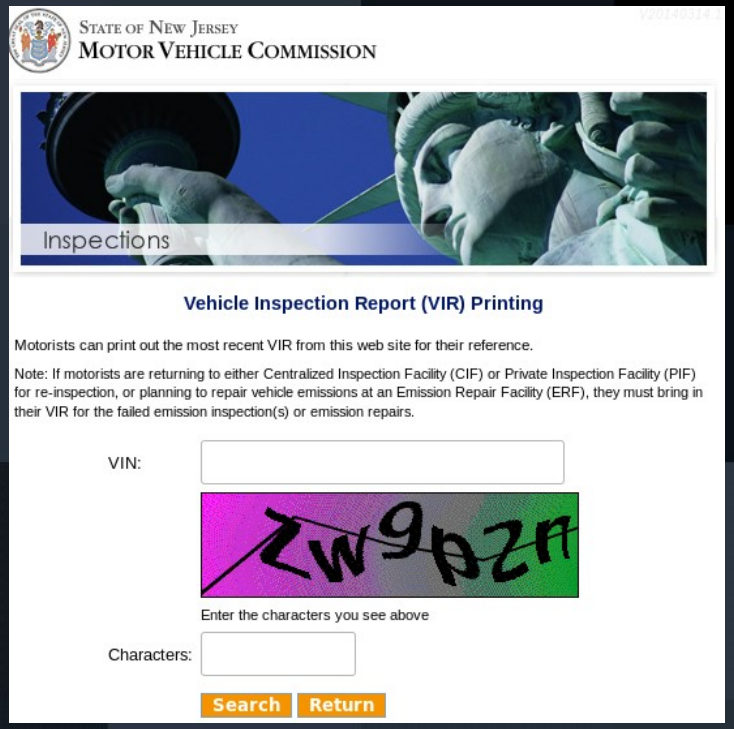
- Wigle.net offers mapping of wireless networks
- Several networks near to Duke's house
  - One may be his home network
- Each dot is a record of a network



Vehicles

- Government records of auto sales gave us the VIN to Duke's BMW and photos gave us his plates
  - Inspection reports
  - Traffic tickets
  - Sale history





Hobby Time

- Duke is an avid Dog Show enthusiast.
- He posts a lot in members-only forums at showdog.com
  - Learned about upcoming events he would be attending
  - Talked about some veterinary issues
  - Forum also shows us when he is active based on posts but some forum software shows users who are just visiting

Tracking Duke

- Geotagging is dangerous, just ask the U.S. Military
- Built a profile of Duke's movements based on social media posts
  - Comprehensive map which included recent concert visits and parts of daily routine

Fitness tracking app Strava gives away location of secret US army bases

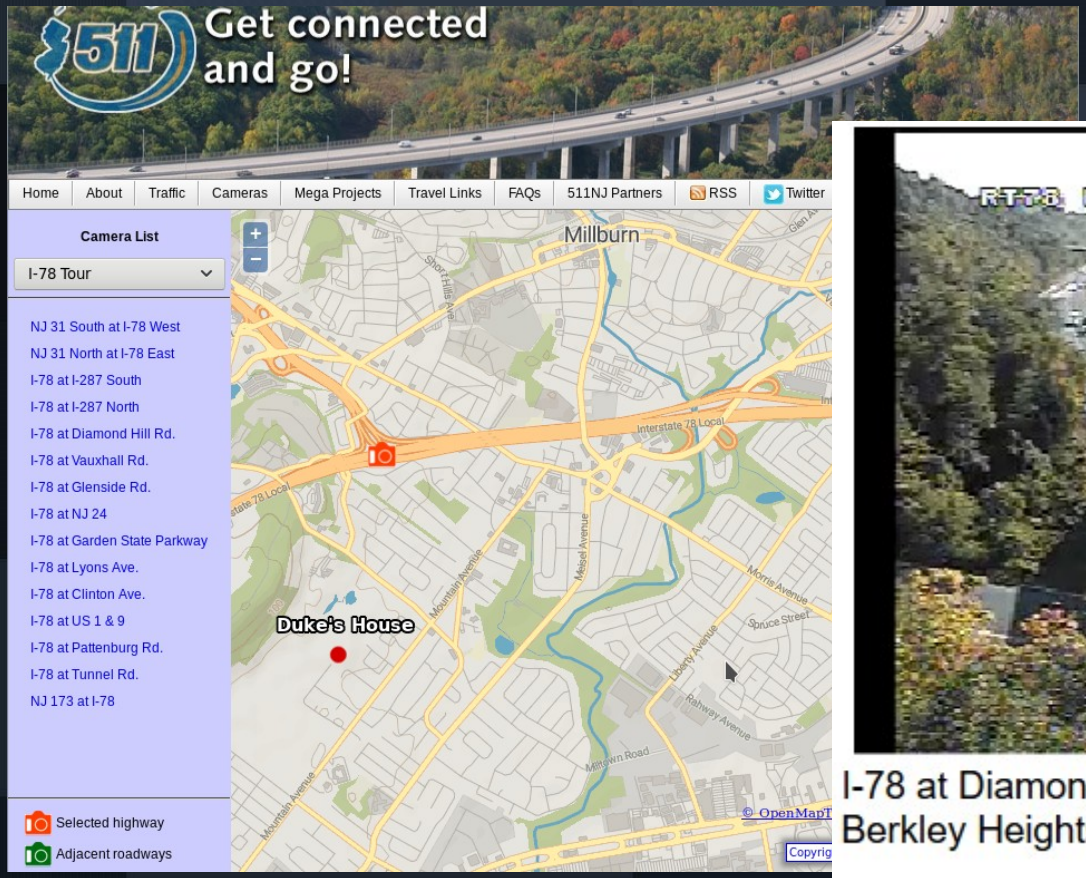
Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

▲ A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap

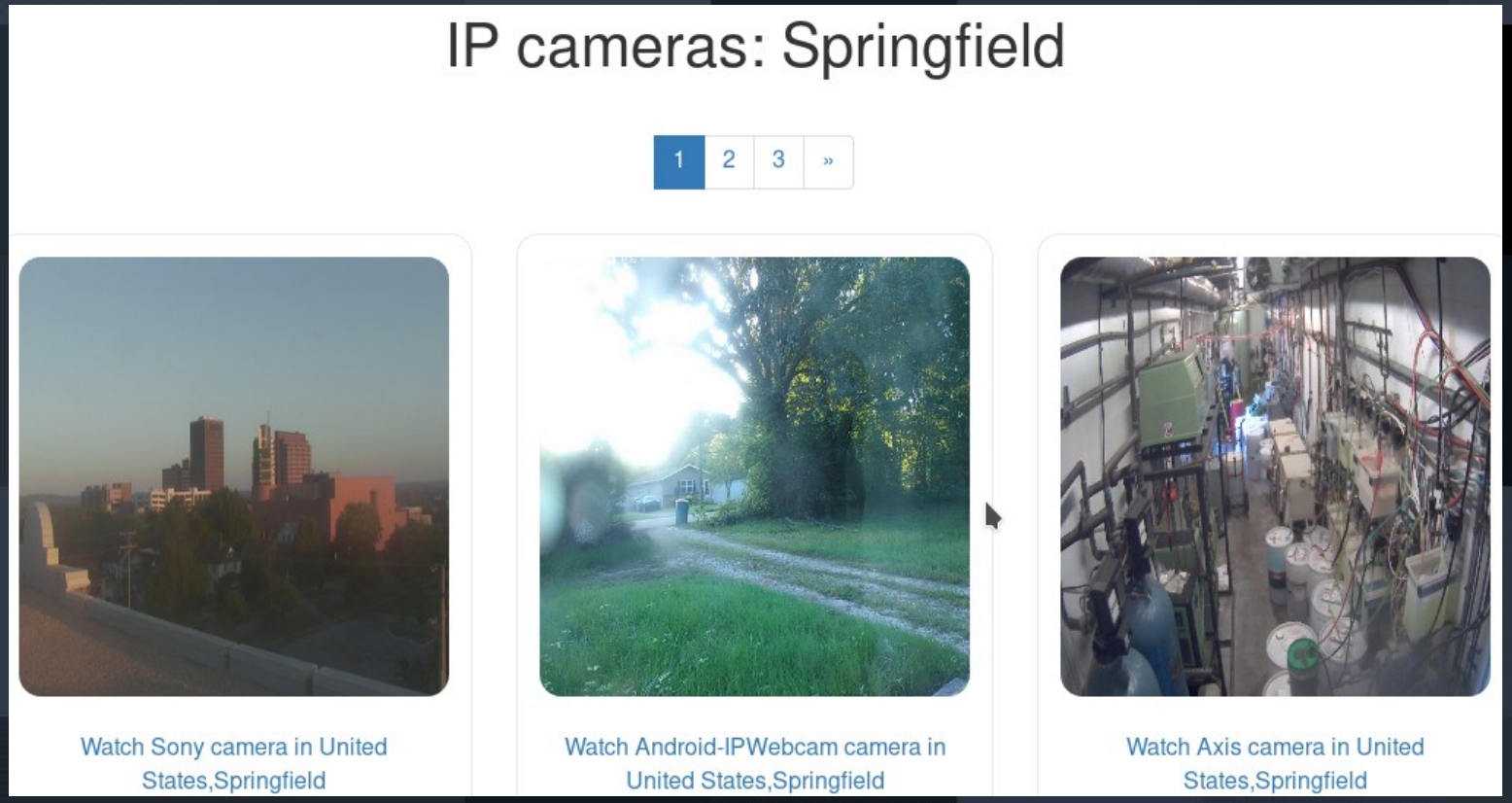
There are Cameras EVERYWHERE

- NJDOT runs traffic cameras for highways
- Since we know what Duke's car looks like, we could watch him commute



No, REALLY EVERYWHERE

- Insecam.org is a list of open IP Camera streams
- Luckily for Duke, he lives in Springfield which is a very common city name



Last Stages

- In the last hours of our reconnaissance we sent Duke an e-mail to his labradoodle4__life@gmail.com address
- He replied, which gave us his IP address
  - Revealed his Cellular provider via e-mail headers
  - Same method can be used to determine home internet provider
  - Good for further Social Engineering attacks

Summary

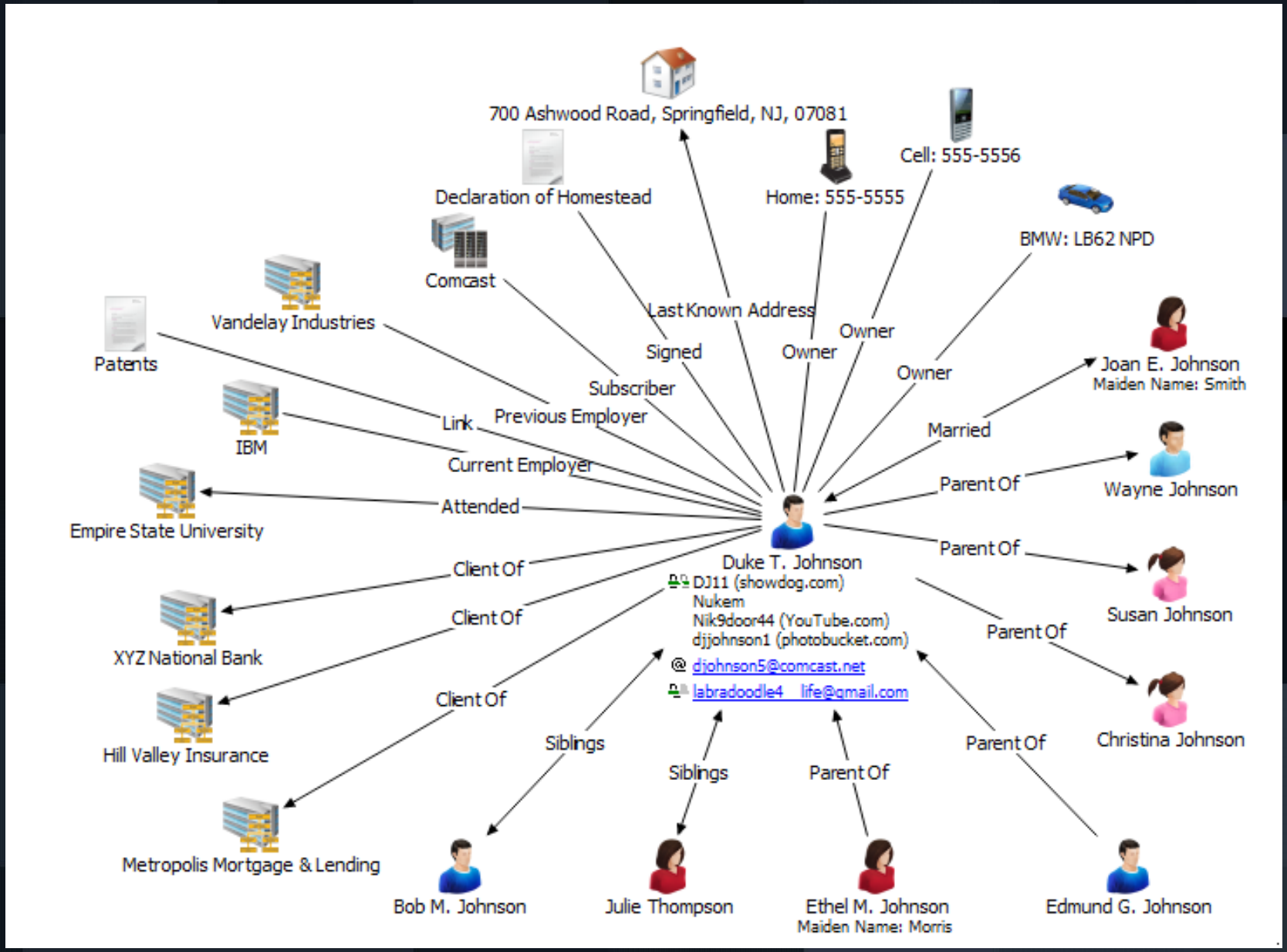
- We’ve turned his name into:

Associations	Assets	Locations	Times
Family & Pets	Home	Home Address	Hours of Work
Friends	Vehicles	Office Address	Visits/Posts to Forums
Colleagues	Devices	Business Travel	Business Travel Schedule
Employers	Banks & Credit	Hobby Travel	Hobby Travel Schedule
Businesses		Children’s Schools	
Artists			
Hobbies			
Schools			

Organizing

- Organization is critical to OSINT, especially with a team
  - Need to track:
    - What you found
    - Where you found it
    - Quality of the source
- We used IBM i2 to organize because it was free for us
  - Maltego CE is a great free option
  - Used by Insurance/LE/Intelligence Agencies for exactly this type of thing
- Enabled teamwork and helped effectively track findings
- Let us make pretty graphs

Simplified Graph



Important Note

- Consider the information in our dossier
- We haven’t left our desks at all and our target is hundreds of kilometers away
  - We have great chairs
- Consider what information we could get if we had a budget / were able to travel
  - Local county records offices
  - Direct drive-by of current property
  - Clear picture of Duke’s work situation
  - Daily habits

Threat Modeling

- Now that we have all this information, what can we do with it?

It’s not “Deliverables”, it’s Delissio!

- Our deliverable was a 50-page paper including references and bibliography
  - Developed approximately 50 scenarios
  - Proposed mitigation for many of them
  - Working on releasing to public
- The fun part – where we get to play bad guy and imagine what could be done with all this information we gathered

Example Threats

- Watering Hole Attack
  - Phishing attack against Duke via his hobby websites or other frequented websites
  - Example: User posts “hey, I have a labradoodle and am interested in knowing about this particular show <link to malicious site>”
- Spearphishing Attack on our Target
  - Directed phishing attack using any of the info we’ve gathered
  - Example: “Hi Duke, it’s Bob from Air Group, we got a recall notice on a part we installed when we were doing the furnace work last year. Can you fill out the serial number on the side of the furnace in this site and let us know if it comes back as needing replacement ASAP? <malicious link>
    The part in question may fail and leave you guys without heat so we want to get this taken care of quickly.
    Regards, Bob”

Example Threats II

- Spearphishing Attack on people working with our Target
  - Example Attack: “Hi Pauline, I was speaking with Duke about having you guys submit a bid on a request for tender. Since he’s away in Cleveland for his dog show this week he asked me to just pass it along to you. The details are available at: <malicious link>. The RFT closes at the end of the week – I hope that’s enough time.”
- Device Theft
  - Attacker knows Duke’s upcoming travel schedule thanks to his dog show hobby. Using this info, attacker arranges to show up in person and steal phone/laptop, plant rootkits, clone work badge/access card.
    - Alternatively, attacker breaks into Duke’s home & steals laptop, etc.
- Swatting

How to Protect Yourself: Average Jane/Joe Edition

- Don’t re-use aliases across systems
  - Definitely don’t reuse passwords
    - Passwords shouldn’t contain things like pet’s names, family members’ names, etc.
- Lock down all permissions on social media
- Go through old social media posts and clean up
- Don’t post when you’re traveling via social media
- Turn off geotagging everywhere
  - There are phone apps that will strip metadata from photos as you take them/share them
- Secure your home network/IoT devices
- Ignore/beware of e-mails or direct messages that ask you to urgently click on links

How to Protect Yourself: Paranoid Security Person Edition

- Follow the previous slide, plus:
- Separate your online aliases
  - Unique e-mails and accounts per “identity”
  - Avoid cross-referencing / sharing the same things on multiple accounts
- Disable all location tracking
- Don’t use anything cloud-based (ha!)
- Set up VPN connectivity on your mobile device
  - Always be connected to it
- Use TOR for routine browsing

How to Protect Yourself: Hermit Edition

- Realize people can still find information about you regardless of how disciplined you are
  - The price of modern existence seems to be the loss of true anonymity

- Solve this all by finding a cave in a remote area and living in solitude for the remainder of your days
- Hope no satellites or drones caught you walking there!

Questions?

References & links follow within the slides!

Slides are available at: https://ibm.biz/OSINT101

References – Articles

- LifeLock executive victim of identity theft 13 times
  - https://www.wired.com/2010/05/lifelock-identity-theft/
- Securitas CEO victim of Identify Theft
  - https://www.bloomberg.com/news/articles/2017-07-12/securitas-ceo-declared-bankrupt-after-his-identity-was-stolen
- Fitness tracking app Strava gives away location of secret US army bases
  - https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
- Geotagging poses security risks
  - https://www.army.mil/article/75165/geotagging_poses_security_risks
- Real Future: What Happens When You Dare Expert Hackers …
  - https://www.youtube.com/watch?v=F78UdORIl-Q
- Password Do’s and Don’ts
  - https://krebsonsecurity.com/password-dos-and-donts/

References – Tools

- OSINT Framework
  - https://osintframework.com
- Recon-ng
  - https://bitbucket.org/LaNMaSteR53/recon-ng
- Haveibeenpwned
  - https://haveibeenpwned.com
- Wigle (Wifi map)
  - https://www.wigle.net
- Insecam
  - https://www.insecam.org
- Maltego Community Edition
  - https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php
- IBM i2 Analyst's Notebook
  - https://www.ibm.com/ca-en/marketplace/analysts-notebook

References – NJ Resources

- NJ Geoweb (Aerial Surveys)
  - https://www.nj.gov/dep/gis/geowebsplash.htm
- County Records
  - https://www.nj.gov/state/archives/catcounty.html
- NJ Court Records
  - https://njcourts.gov/courts/superior/copiesrecords.html
- Real Estate for Sale (Tons of sites)
  - https://www.zillow.com/nj
- DOT Cameras
  - http://www.511nj.org/

References – Ontario Resources

- Ontario Court of Justice
  - http://www.ontariocourts.ca/ocj/search/
- Library and Archives Canada
  - https://www.bac-lac.gc.ca/eng/discover/genealogy/places/Pages/ontario.aspx
- Real Estate for Sale
  - https://www.realtor.ca
- Vehicle VIN lookup, if it's had to pass DriveClean
  - http://www.driveclean.ene.gov.on.ca/ONPublicWeb/pages/vir/vehSearch.jsf?LOCALE=en_CA
- MTO Cameras
  - https://511on.ca/cctv

References - Research

- NY Cab trip data deanonymized
  - https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546
  - https://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/
- Unique in the shopping mall: On the reidentifiability of credit card metadata
  - http://science.sciencemag.org/content/347/6221/536.full#ref-26
  - https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data