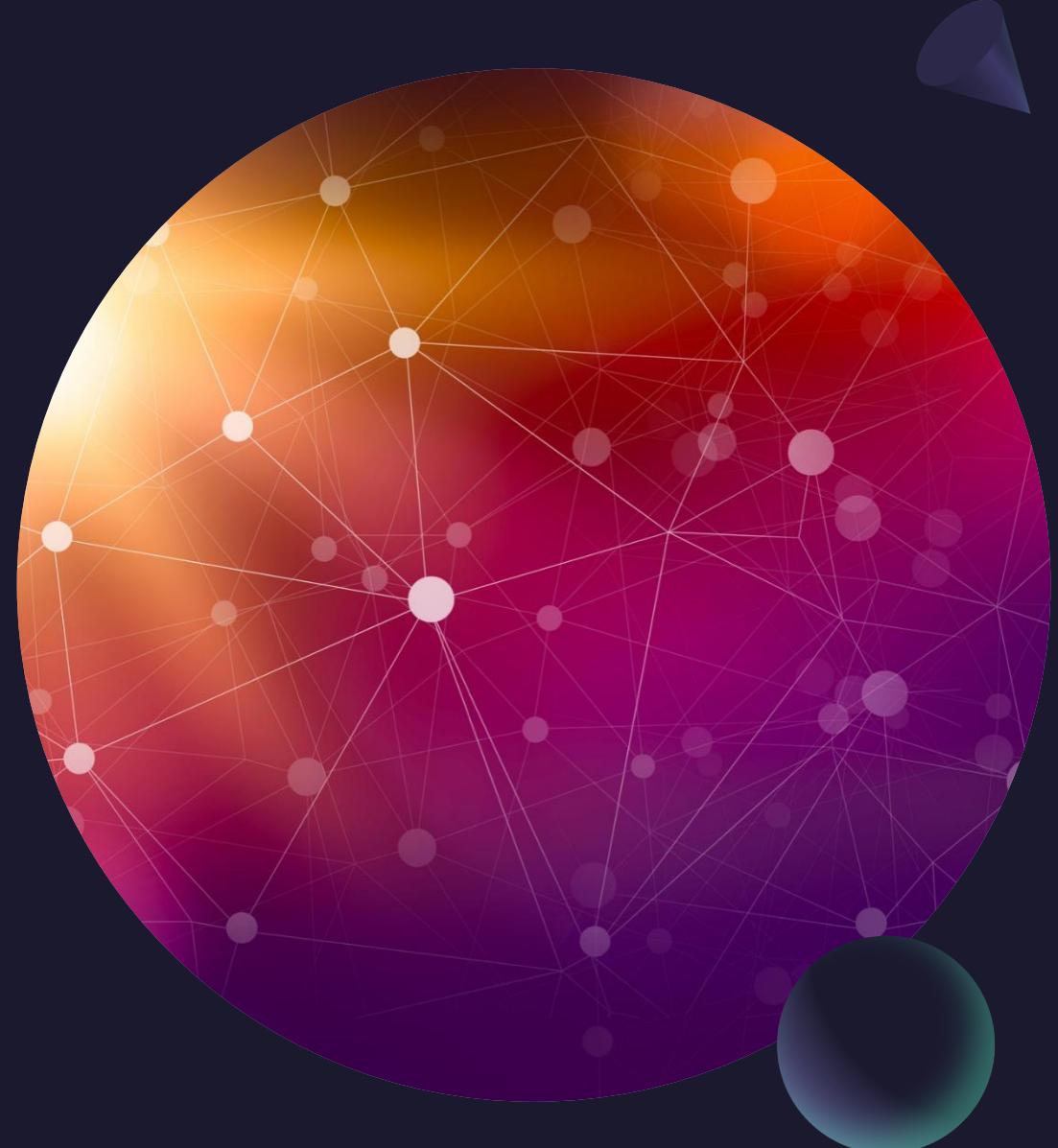


Know Thyself:

Using OSINT to Understand Your Digital Footprint

Michael Miller



Agenda

- Introduction
- Definitions
- Your Digital Footprint
- Understanding Impact
- OSINT
- Threat Modeling
- Controlling Your Exposure



Disclaimer & Caveats

- This is a **PRIVACY** focused presentation
- This is not an OSINT presentation, though we will be discussing some OSINT techniques
- **Please use this information responsibly**



WHOAMI

- Manager, Cybersecurity Platform Engineering @ Cardinal Health
- 11+ years in IT & Cybersecurity for a variety of industries
- BS Cybersecurity & Information Assurance | AAB Network Administration & Computer Programming
- CCSP, SSCP, CEH, ECES, CySA+, Security+, Network+, A+, Project+, CCFR, CCFA
- Tech and DIY enthusiast who enjoys spending time with family and grilling



Who Are You

- Security Professionals?
 - Hiring Managers?
 - Students?
 - Lost?
- 

Definitions

- OSINT – Open-Source Intelligence – information that is public and generally freely available
- Digital Footprint – your digital data trail of your activities and behaviors on the Internet that is left either directly through your interactions or through third party sources
- Threat Modeling – evaluating what you are trying to protect, and what you are trying to protect it from



Digital Footprint



Digital Footprint

- Active Digital Footprints

- Knowingly created
- Social media postings
- Images and videos shared
- Shopping activities
- Activity on websites

- Passive Digital Footprints

- Involuntarily created
- Geolocation data
- Web analytics and web browsing history
- Internet service logs

- Difficult, if not impossible, to remove
- Can impact all areas of life
 - Reputation and credibility
 - Employment opportunities
 - Education opportunities
 - Family life
 - Identity theft & fraud



Data Points



- Email addresses
- Usernames
- Social media accounts
- Social media postings
- Phone numbers
- Real names
- Family members and associates
- License and vehicle information
- Residential history
- Geolocation data
- Employment history
- Shopping activities and history
- Web browsing history
- DoB and SSN
- Communication messages
- Pictures and videos
- Medical history
- Financial history
- Credit/debit card numbers
- Passwords
- Dating Information
- Political affiliations
- Criminal record

Understanding Impact

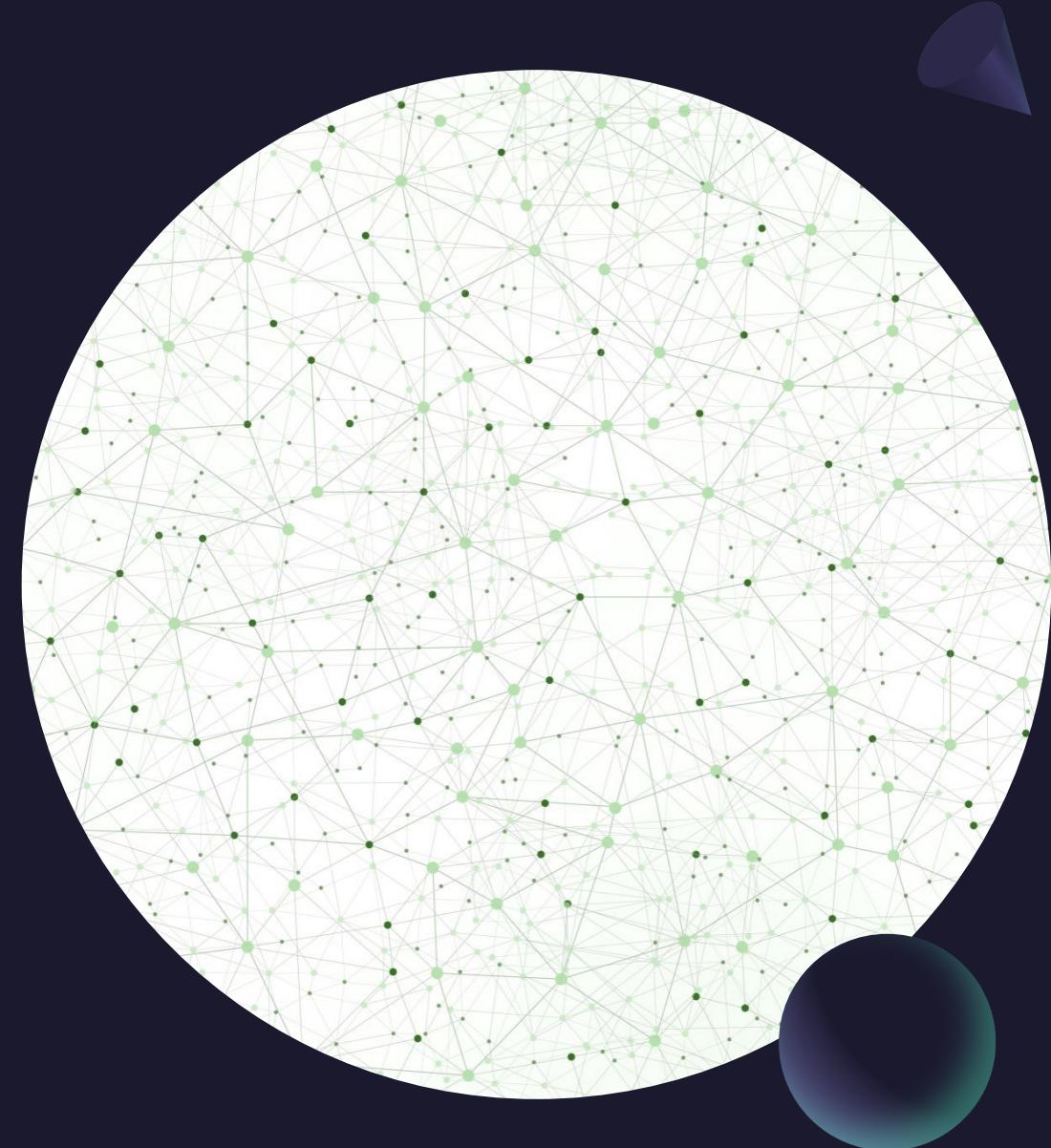
HOW CAN THIS INFORMATION BE USED AGAINST ME?

- Targeted advertising
- Identity theft
- Phishing attacks
- Fraud
- Extortion
- Family challenges
- Reputation damage
- Credibility damage
- Employment challenges
- Education challenges
- Deep fakes
- Stalking/cyberstalking



OSINT

Dusting for your footprints



Search Engine OSINT

- Google Yourself

- Quotations "Michael Miller" vs "Michael" "Miller"
- Search operators
 - Site = "site:facebook.com"
 - Conditional operators = AND OR
 - Wildcard = *
 - Range = "..." ("2020...2023")
 - Filetype = "filetype:docx"
 - In Text = "intext:keywords"



- Bing and other search engines

Social Media OSINT

- Facebook/Instagram
- LinkedIn
- Twitter
- Snapchat
- TikTok
- Reddit
- Tinder
- Pinterest
- Discord
- Craigslist
- eBay
- Amazon



Image OSINT

- Google Reverse Image Search
 - <https://images.google.com/>
- TinEye
 - <https://tineye.com/>



Identity OSINT

- People Search Engines

- <https://www.whitepages.com/>
- <https://www.spokeo.com/>
- <https://www.truepeoplesearch.com/>

- NameCheck

- <https://namechk.com/>



Data Breaches

Have I been Pwned

(<https://haveibeenpwned.com/>)



'--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pwned?



DoorDash

In August 2022, the food ordering and delivery service DoorDash disclosed a data breach that impacted a portion of their customers. DoorDash attributed the breach to an unnamed "third-party vendor" they stated was the victim of a phishing campaign. The incident exposed 367k unique personal email addresses alongside names, post codes and partial card data, namely the brand, expiry data and last four digits of the card.

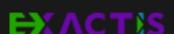
Breach date: 2 August 2022

Date added to HIBP: 7 January 2023

Compromised accounts: 367,476

Compromised data: Email addresses, Geographic locations, Names, Partial credit card data

[Permalink](#)



Exactis

In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

Breach date: 1 June 2018

Date added to HIBP: 25 July 2018

Compromised accounts: 131,577,763

Compromised data: Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages

[Permalink](#)

Breath!

What can we do about it?



Digital Footprints - Not All Bad

- Social Media Influencing
- Networking
- Building your “brand”
- Career building
- Community Outreach





thaddeus e. grugq 🌻 thegrugq@infosec.exchange
@thegrugq

...

Your threat model is not my threat model.



3:42 AM · May 15, 2017

Threat Modeling

- Three main components: assets, threats, and protection mechanisms
 - What are you trying to protect
 - What are you protecting it from
 - How are you protecting it
- Varies widely from individual to individual
- Be realistic

Controlling Your Exposure

- Compartimentalization
- Think before you post
- Eliminate unnecessary accounts
- Opt-out wherever possible
- Request data removal whenever it fits your threat model
- When in doubt redact



Internet/Web Presence

- Consider using different web browser profiles, or web browsers for different purposes
- Consider separate email accounts for different purposes
- Use privacy aware extensions (e.g. Ublock Origin)
- Block unnecessary cookies
- Use a VPN whenever possible
- Use a specialized DNS server and DoH whenever possible
- Limit information shared on social media

Summary

- Your digital footprint is composed of voluntary and involuntary activity data
- You cannot fully remove it, but you can understand what's there, and in some cases request removal of certain pieces of information
- Determine your threat model
- Take control of your active digital footprint
- Take steps to limit your passive digital footprint by being conscious of online activities, compartmentalizing, and using privacy focused extensions and a VPN



Thank You

Michael Miller

mmiller.netsecdev@gmail.com

