KB4-CON

What's New on the Dark Web

by Colin Murphy, Special Operations Engineer

KnowBe4

>whoami

Colin Murphy, CISSP, CEH

- My job title is almost as cool as my job.
- Worked at KnowBe4 for 2 years, customer for 3 years.
- Spend majority of time researching attack vectors, hunting down breaches, and working on various projects to help improve our products.
- Collector of security tools off of GitHub.

Recap of KB4CON 2018: Breaches

- In the past two years we have seen a major shift towards focusing more closely on data breaches.
- The public is more aware of breaches and the consequences.
- Password spraying resulting in lateral attacks on other services
- Better organized data, correlation of breach data
- The trading and buying of breach data on private forums/membership platforms.
- Crowd sourced hash cracking turning billions of hashes into plaintext

Defining the various web's

SURFACE WEB

General websites, can be found via search engines (pastebin, google searches, social media, blogs)

DEEP WEB

Requires authentication to access content (forums, membership sites- we leak info, discord, government websites)

DARK WEB

Requires Darknet to access: tor, I2P, Freenet, Zeronet – Web pages/content only accessible via specialized network tools. Has its own search engines, social media websites, web market places.

The natural flow of “loot” out of the dark web

Dark Web

Traded amongst small private groups. Sometimes kept secret for years. Unknown threat exposure.

The natural flow of “loot” out of the dark web

Traded amongst small private groups. Sometimes kept secret for years. Unknown threat exposure.

Information is now available to the largest group of cyber criminals. Wide spread attack campaigns

The natural flow of “loot” out of the dark web

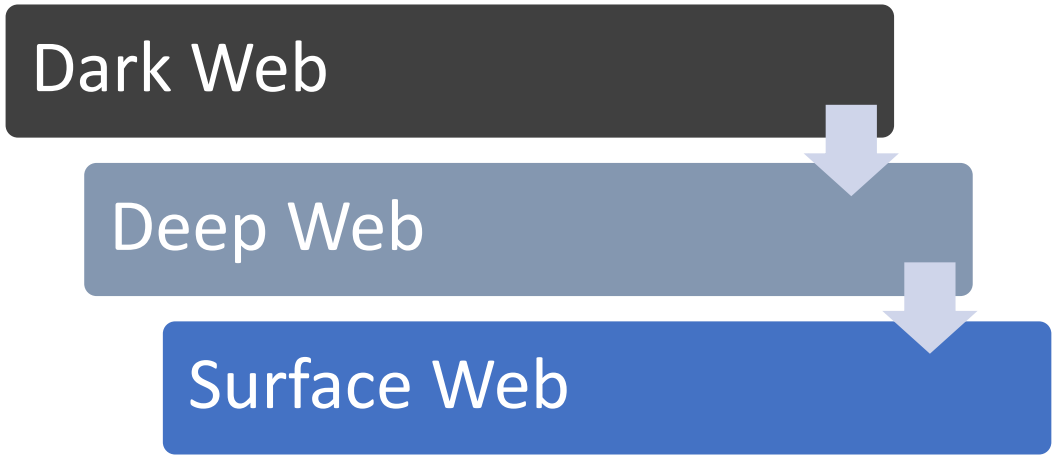
Traded amongst small private groups. Sometimes kept secret for years. Unknown threat exposure.

Information is now available to the largest group of cyber criminals. Wide spread attack campaigns.

Information is now public domain. Researchers, marketers, news, and general public can now easily acquire. Exposure becomes disclosure.

The natural flow of “loot” out of the dark web

Key changes in 2019:



Major breaches getting to the surface web faster, more organized.

Blackhats, whitehats, and organizations are actively seeking breach data.

Regardless of skill and intention, everyone is getting access.

It has never been easier to get our information

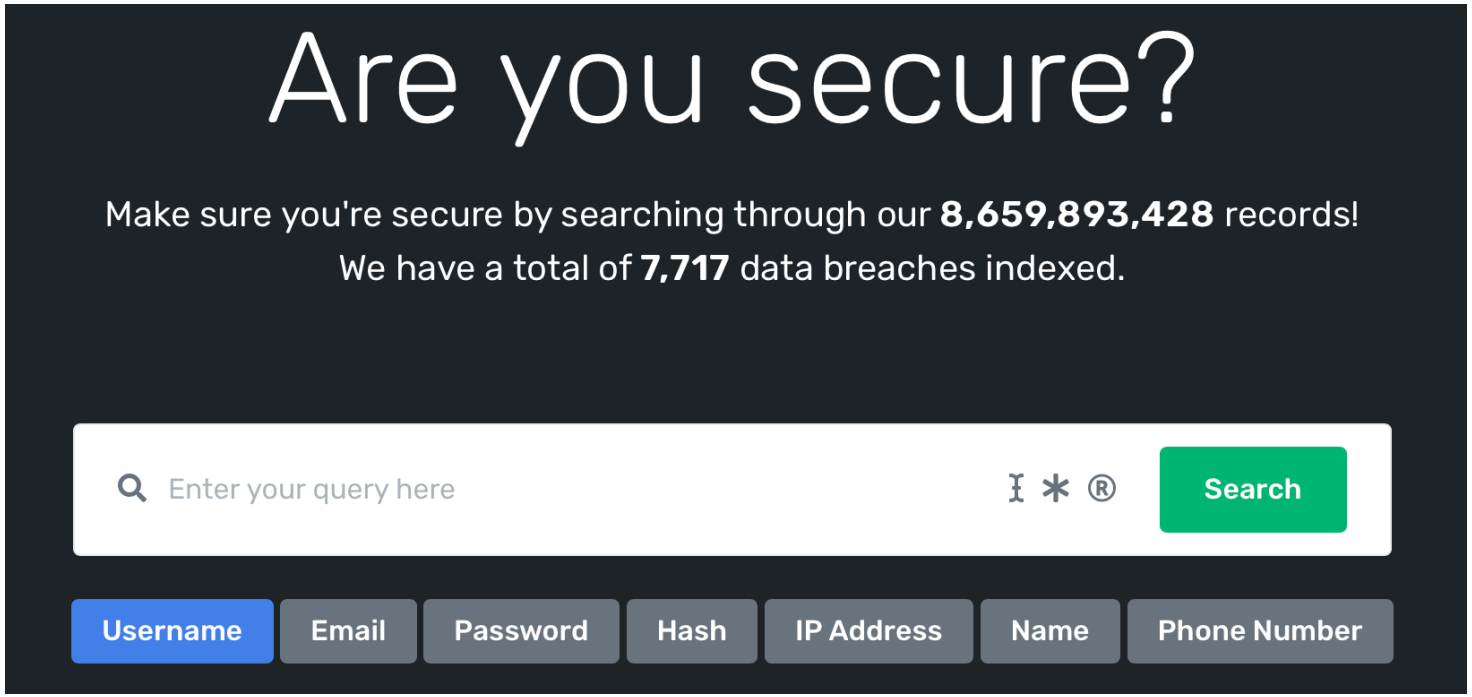
Top 5 major breaches and exposed data types:

Yahoo	Marriot	Adult Friend Finder	eBay	Equifax	The Collection
3 Billion User Accounts	500 Million Customers	412.2 Million Accounts	145 Millions Users	147.9 Million Consumers	25 Billion Records
2013 - 2014	2014 - 2018	October 2016	May 2014	May 2017 – July 2017	January 2019
• Real Names • Email • DOB • Telephone Number • Passwords • Security Questions	• Maintained Access to DB for years • Contact Info • Passports • Travel Info • 100 Million Credit Cards • Possible Source of Attack – Nation State	• 20 Years of Data • Names • Email Addresses • Password	• Hackers Maintained Access for 229 days • Used Employee Credentials • Accessed Account Information	• Several Months of Access • Personal Information: Social Security Numbers, Birth Dates, Addresses, Drivers License Numbers, etc. • 209,000 Had Credit Card Data Exposed	• 2.2 Billion Unique Usernames and Associated Passwords • Creator Cleaned Up and Organized Credentials to Resell to Criminals • Publicly Available for Download and Now Searchable on Several Breach Websites

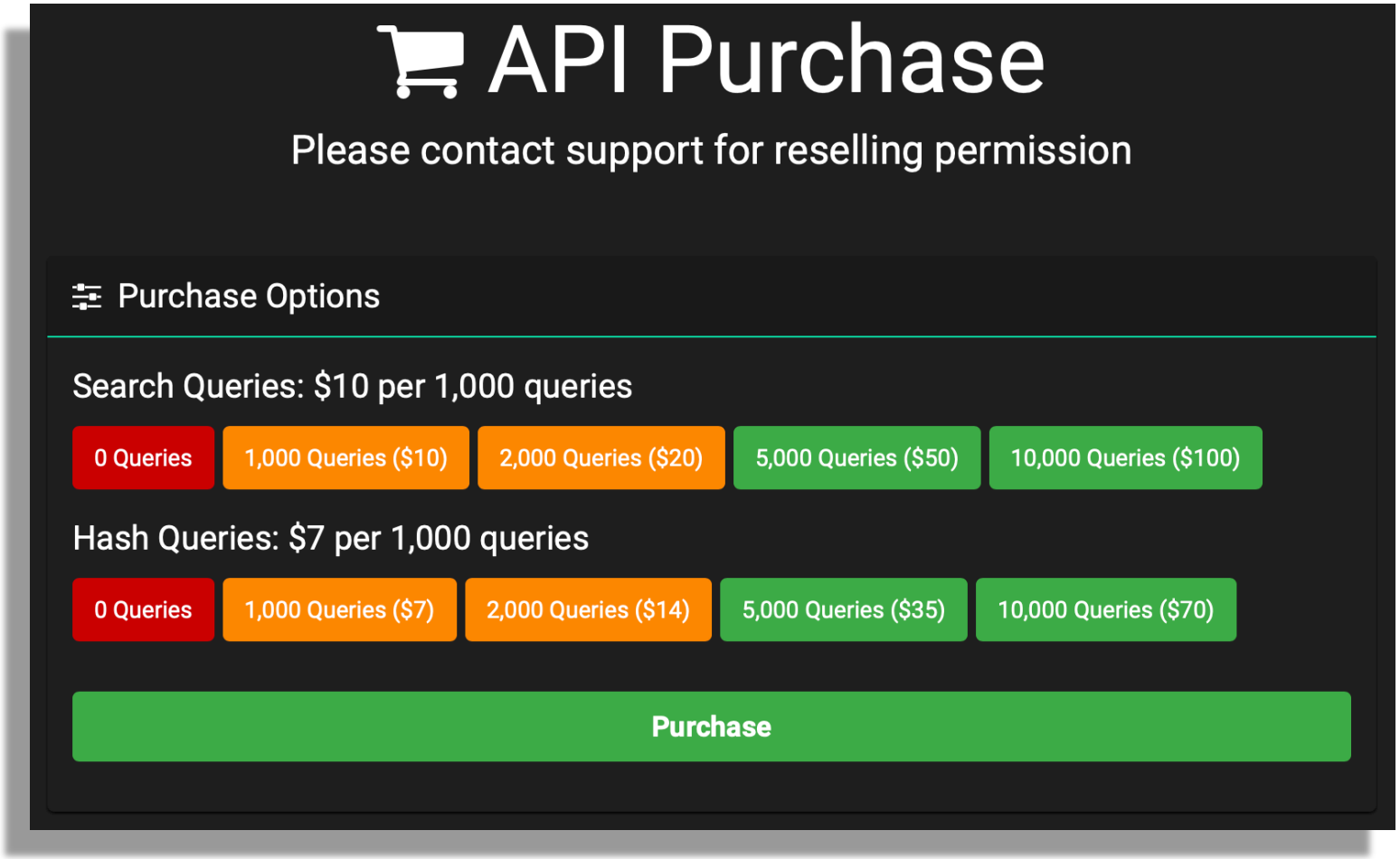
Blackhats turned.. Entrepreneurs?

Last year we discussed a website that imported breached data into a searchable database.

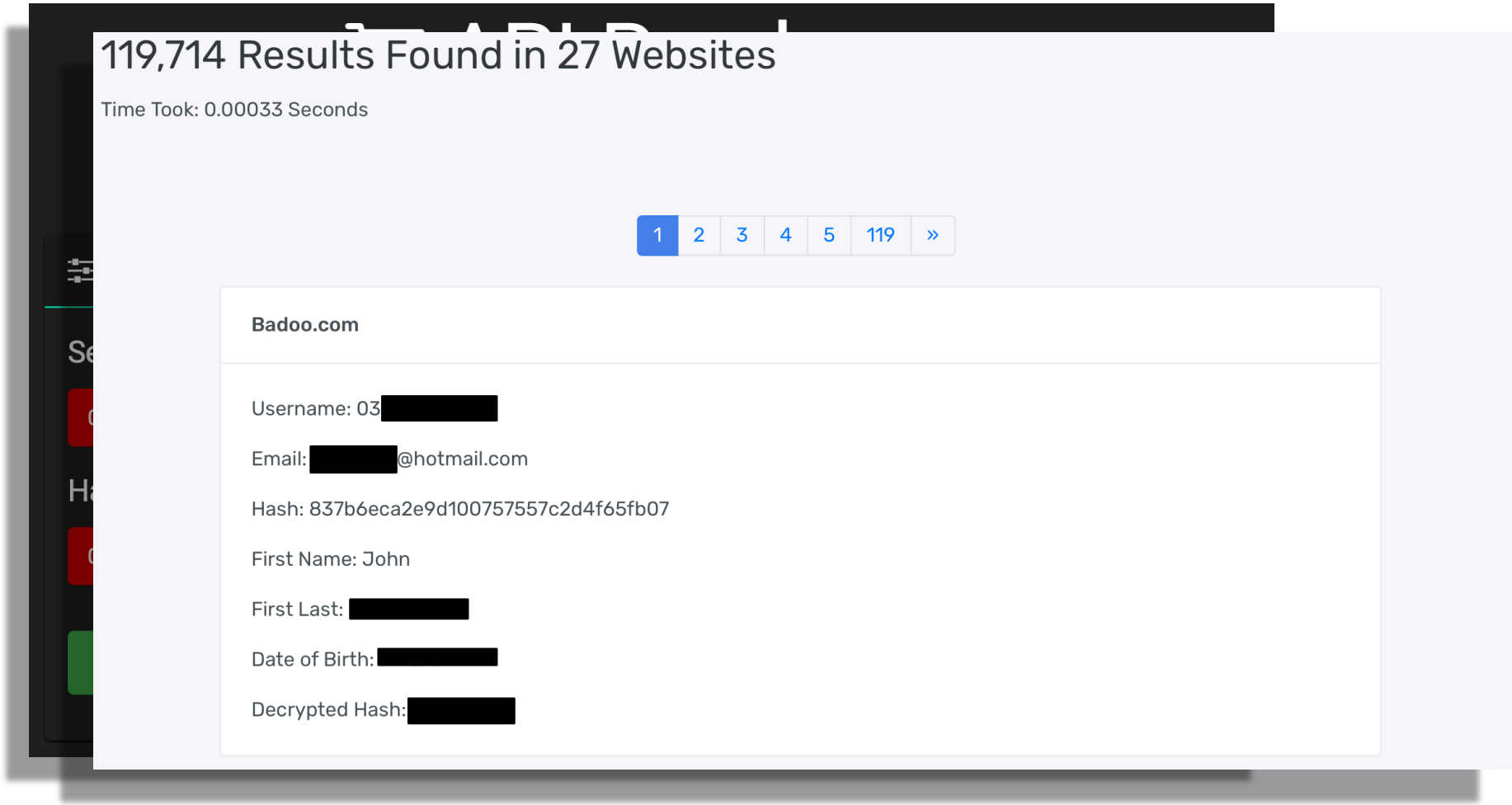
This year, they have rebranded their organization, redesigned their website, and are working harder than ever to import more breach data (from 5 billion to over 8 billion records).



Blackhats turned.. Entrepreneurs?



Blackhats turned.. Entrepreneurs?



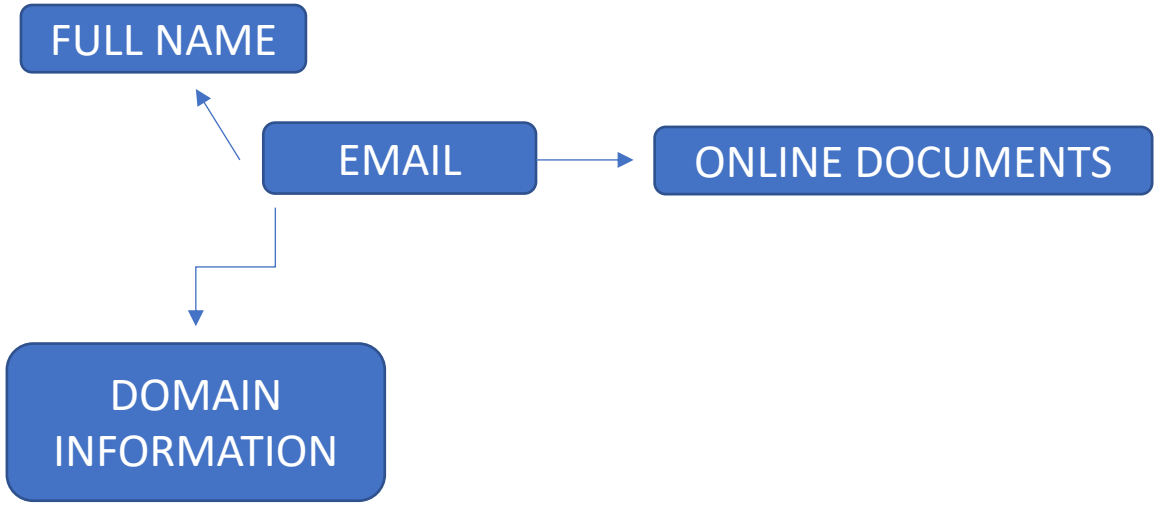
Enough about breaches, lets talk OSINT

OSINT's Role in Social Engineering Attacks:

1. It is information collected from public sources that is free, public, legal.
2. Can be used by anyone for building a profile on a target or subject.
3. General sources of OSINT online
   - Social Media
   - Marketers
   - Public records
   - Web searches
4. Enriched OSINT
   - Breaches (raw form)
   - Collections of organized and cleaned breach data (easily searchable)

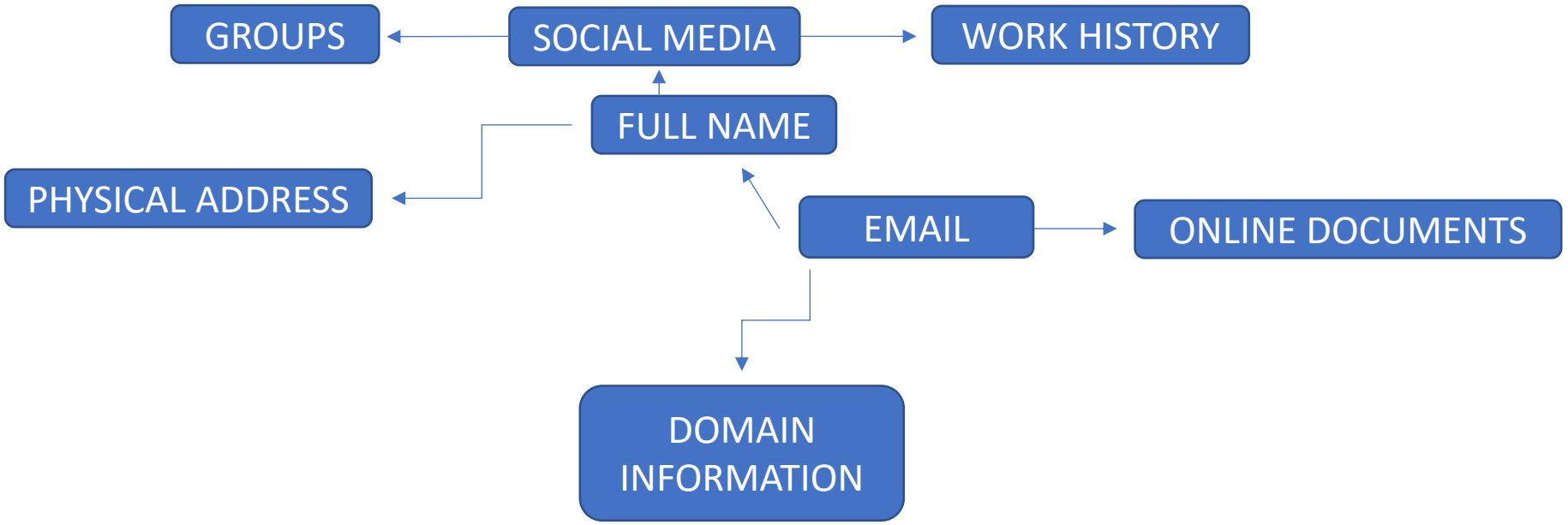
Standard OSINT example:

The below diagram shows the various data points connected to an object. In this case the object is an email address.



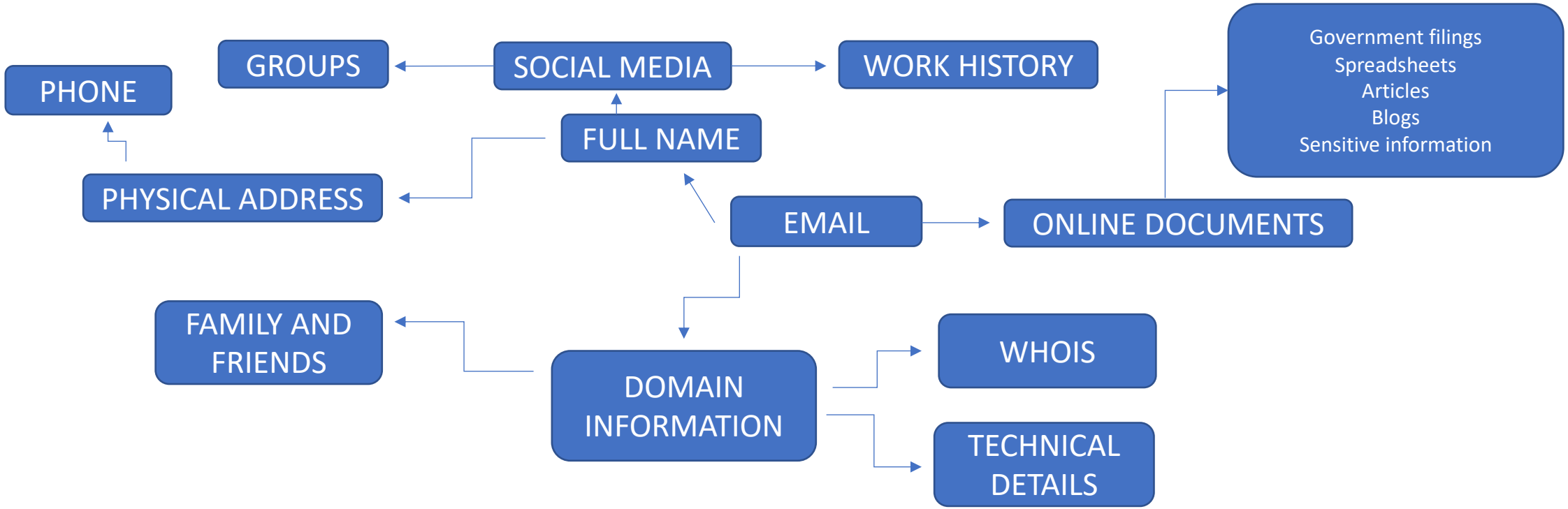
Standard OSINT example:

The below diagram shows the various data points connected to an object. In this case the object is an email address.



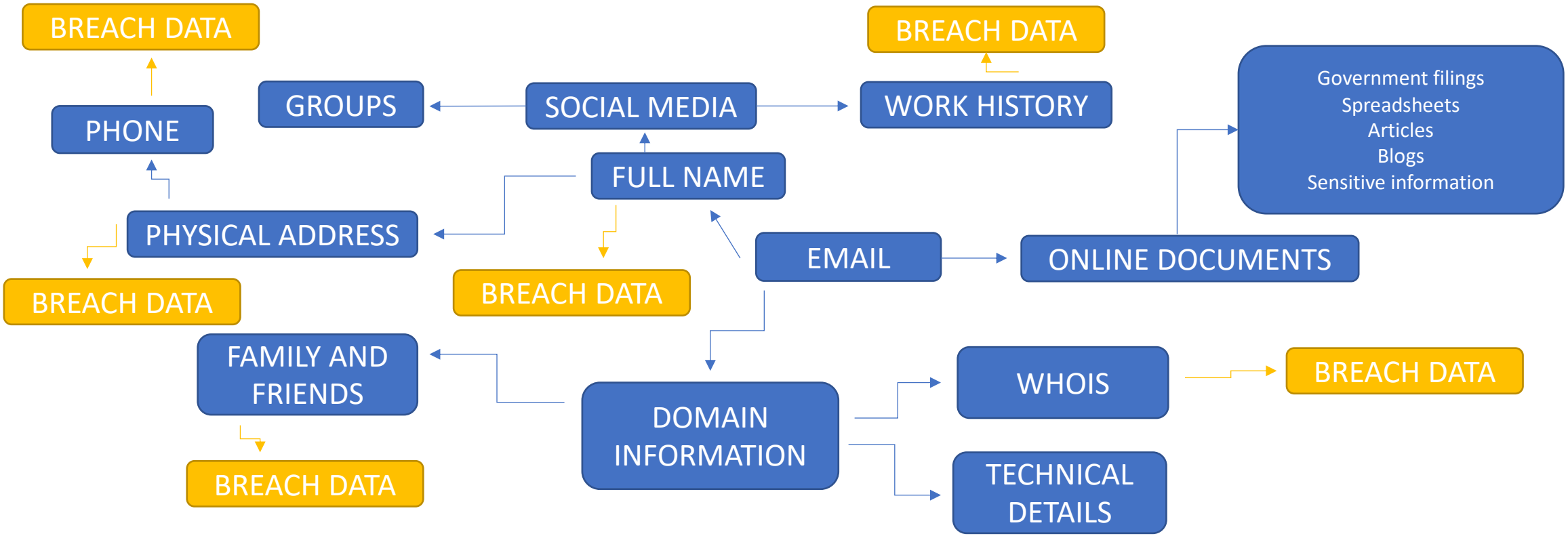
Standard OSINT example:

The below diagram shows the various data points connected to an object. In this case the object is an email address.



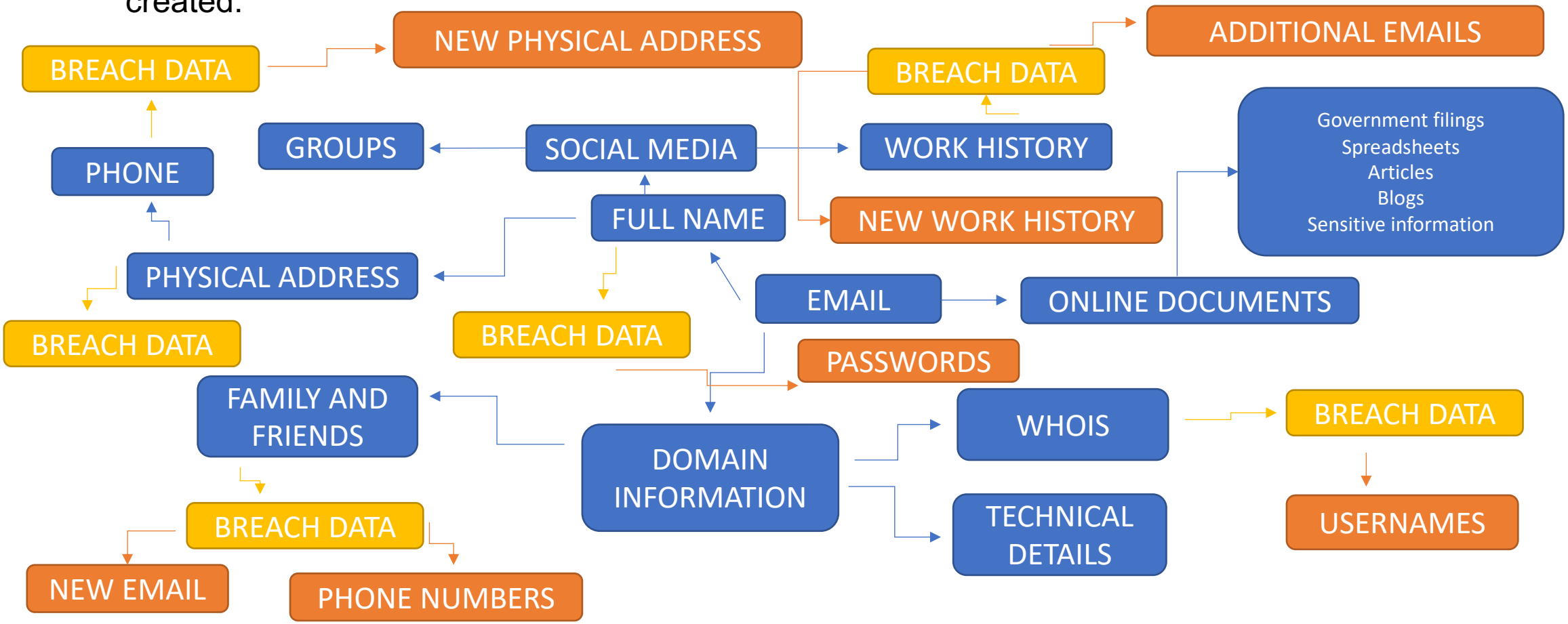
Breach Enriched OSINT example:

Same OSINT information but can be used to dig much deeper into each data point.

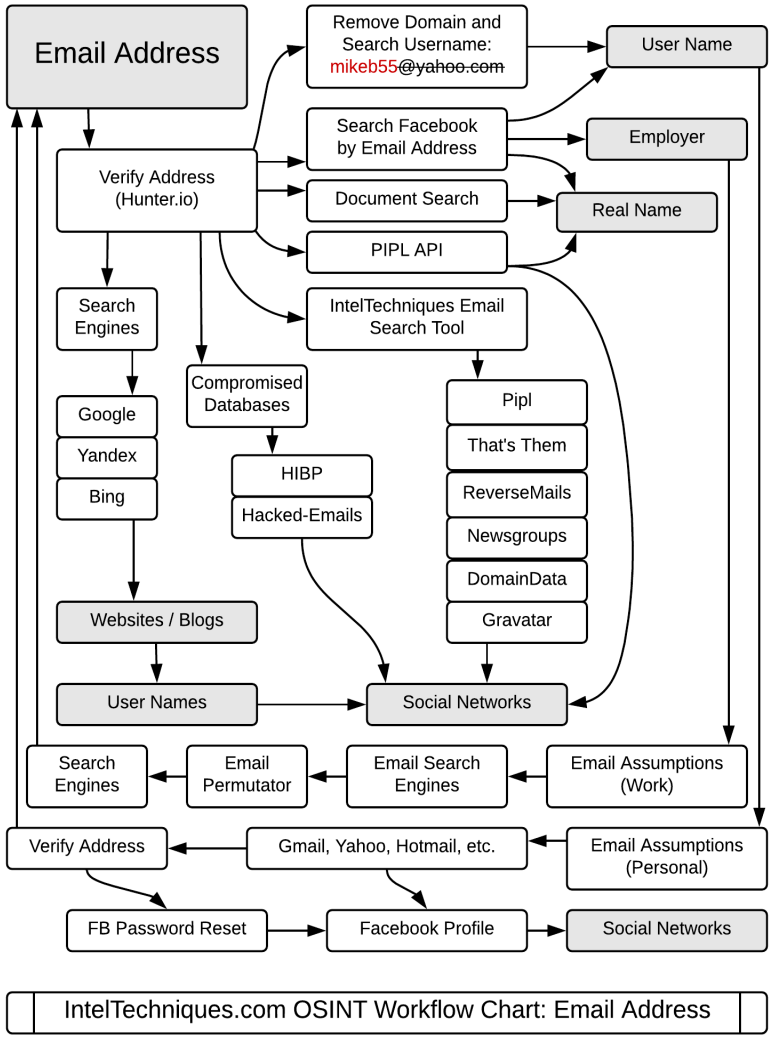


Breach Enriched OSINT example:

This is where things get a bit crazy. For each new data point we recover an entire new graph could be created.



So many sources of information

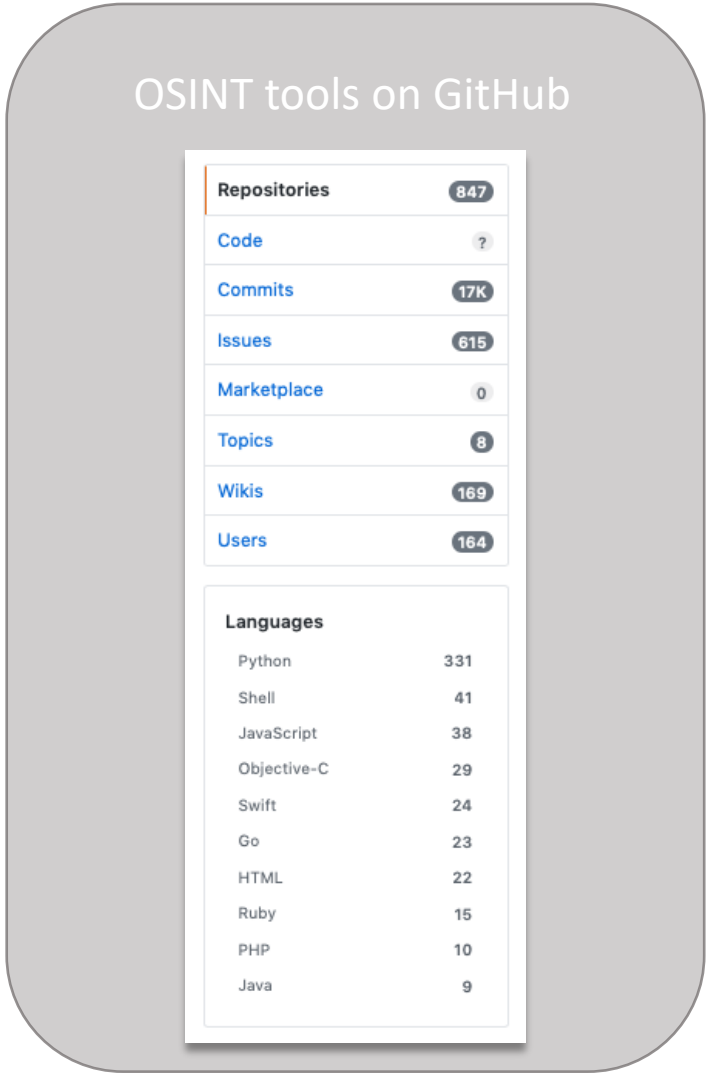


IntelTechniques.com OSINT Workflow Chart: Email Address

Combination of marketer websites, social networks, breaches, and API's.

Additional work flows for other objects (name, address, phone number, location, domain, username)

Blackhats have these same tools plus criminal resources.



Example of what is possible…

60 minutes to get as much as possible using only OSINT + Breaches

- Date married
- Press release quoting where the target was moving from/to.
- Breaches that were tied to email addresses, phone numbers, other names, past jobs
- Groups, hobbies, interests (serves on local chamber of commerce)
- Private documents and reports that should not be public, on company webserver
- Social media, web forums, usernames
- Investment properties with partner under different name
- Family, friends ,coworkers and their social media accounts
- Past phone numbers and physical addresses
- Car loans plus the vin numbers and dates purchased.
- Political donations for past 15 years

With enough time our exposure is limitless.

Statistics from real pentests

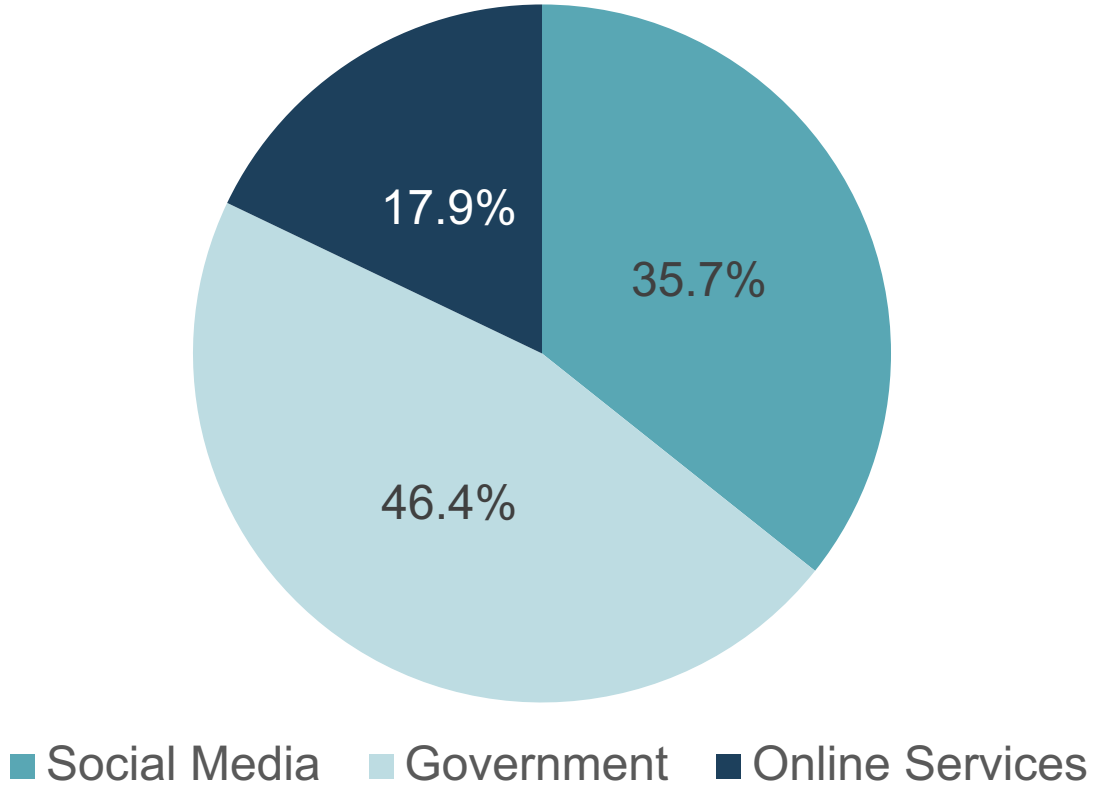
Throughout the tests we used information recovered from OSINT + Breaches to craft realistic spear-phishing attacks.

Top 3 categories that resulted in a failure:

46.4% Social Media

35.7% Government

17.9% Online Services



Spearphish example #1

Call to action to “click”

Real information to build trust

From: ups@ups-alerts.com
Reply-to: ups@ups-alerts.com
Subject: UPS Label Delivery, 1ZDE312TNW00025011

Send me a test email
Toggle red flags

***Do not reply to this e-mail. UPS will not receive your reply.

Important Delivery Information

Delivery Status:	Could not deliver package due to invalid information.
Fix Errors:	CLICK HERE
Please click the above link to correct the errors and we will attempt to re-deliver your package	

Driver Release Location: COULD NOT DELIVER

Original Shipment Detail:

Ship To:

[redacted]

Number of Packages:
1

UPS Service:
UPS 2ND DAY AIR

Weight:
1.0 LBS

Spearphish example #2

Full legal name

”Click” or there will be penalties

Address of an investment property

Different last names on deed

May 8, 2019

Mrs. [redacted]

Due to your updated tax status, a balance is due. Click HERE to view and pay the balance by May 18, 2019 in order to avoid penalties.

Location: [redacted]
Legal: [redacted] BLK G LOT 16
Owners: [redacted] & [redacted]

Kenneth Maun
Collin County Tax Assessor-Collector

Collin County Administration Building
2300 Bloomdale Rd., Suite 2324
McKinney, TX 75071

COLLIN COUNTY
collincountytx.gov

Mitigation

Train your users and increase the difficulty with realistic attacks.

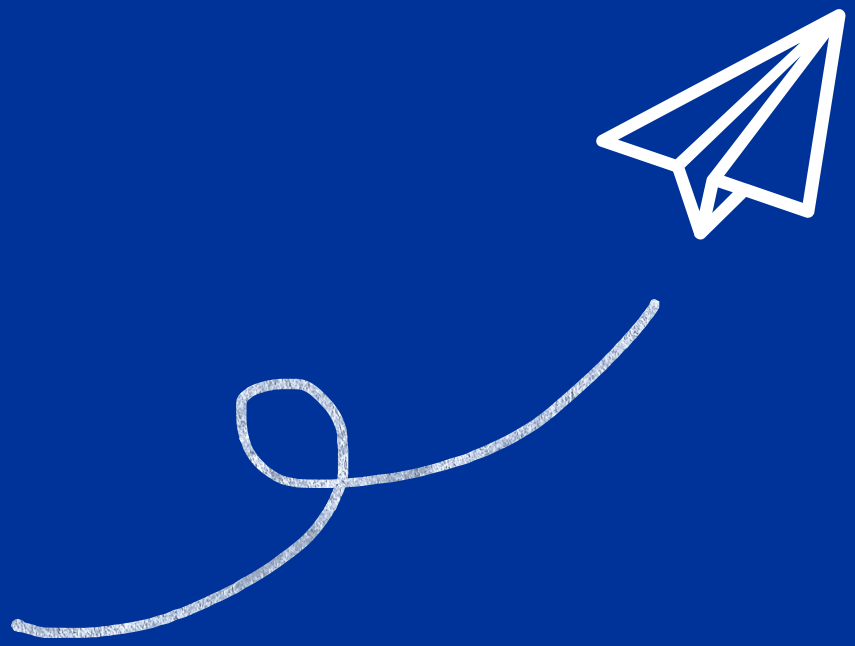
- In KMSAT use placeholders when crating email templates to personalize the phish
- Run EECPro and use the results to craft custom templates
- Target highest risk users

If you are not already doing it, start using OSINT to expose hidden risk.

- Lots of tools on github.com
- Inteltechniques.com
- EECPro (Social media/Breach data)
- Kitploit.com

Use fake information when filling out forms for services you do not intend to purchase.

- Alias email account
- Fake name
- Generic corporate contact number



Key Takeaways

Your attack surface is more public than ever before.

Breaches are supercharging what can be used against us.

Bad guys have access to OSINT tools to automate the research.

Expect social engineering attacks to get more personal.

Can’t delete the data, train your users.

Sources

- https://www.darkowl.com/what-is-the-darknet/
- https://www.inteltechniques.com (OSINT training and tools)
- https://www.wired.com/story/collection-leak-usernames-passwords-billions/
- https://haveibeenpwned.com/ (safest breach website to use)
- https://weleakinfo.com (use at your own risk, blackhat service)
- https://www.kitploit.com/ (steady stream of open source security tools)

Thank You!

Colin Murphy, Special Operations Engineer

KnowBe4