[The Art of Doxing]

[By: Deric Lostutter (KYAnonymous)

Table of Contents

What is Doxing?

DOX -

däks/

verb
informal
gerund or present participle: **doxing**

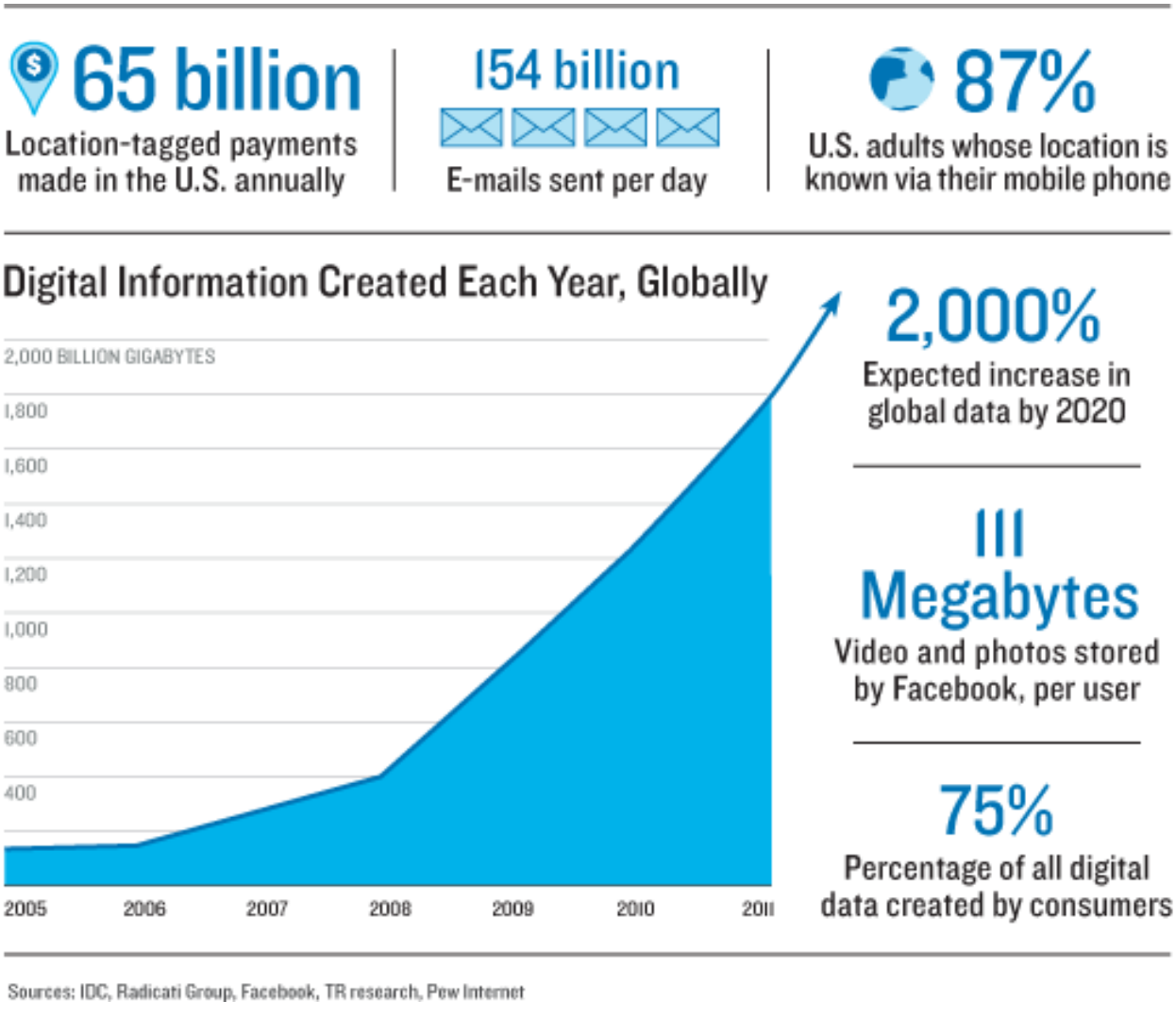
1. search for and publish private or identifying information about (a particular individual) on the Internet, typically with malicious intent.

Highlights

- Hackers and amateur detectives alike can harvest the information from the internet about individuals. A basic Google search can yield results. Social media platforms like Facebook, Twitter, Tumblr, and Linkedin offer a wealth of private information, because many users have high levels of self-disclosure (i.e. sharing their photos, place of employment, phone number, email address), but low levels of security. It is also possible to extrapolate a person's name and home address from a cell-phone number, through such services as reverse phone lookup

  The term "dox" entered mainstream public awareness through media attention attracted by Anonymous, the Internet-based group of hacktivists and pranksters who make frequent use of doxing, as well as related groups like AntiSec and LulzSec.
- In December 2011, Anonymous exposed detailed information of 7,000 members of law enforcement in response to investigations into hacking activities.
- In November 2014, Anonymous began releasing the identities of members of the Ku Klux Klan.This was in relation to local Klan members in Ferguson, Missouri, making threats to shoot anyone who provoked them while protesting the shooting of Michael Brown. Anonymous also hijacked the group's Twitter page, and this resulted in veiled threats of violence against members of Anonymous.

- In April 2015, Anonymous made threats to release the identities of the Vineland Police Department and the Cumberland County Prosecutors Office. The threat was made over at an Anonymous associated youtube channel, and is still an evolving event. The threat was in regards to a Vineland, NJ man who died in custody.
- In March 2015, former MLB pitcher Curt Schilling used doxing to identify several people responsible for "Twitter troll" posts with obscene, sexually explicit comments about his teenage daughter. One person was suspended from his community college, and another lost a part-time job with the New York Yankees



The Growth of Data

Here's what happened. First, the amount of data created each year has grown exponentially: it reached 2.8 zettabytes in 2012, a number that's as gigantic as it sounds, and will double again by 2015, according to the consultancy IDC. Of that,

about three-quarters is generated by individuals as they create and move digital files. A typical American office worker produces 1.8 million megabytes of data each year. That is about 5,000 megabytes a day, including downloaded movies, Word files, e-mail, and the bits generated by computers as that information is moved along mobile networks or across the Internet.

Where do we begin? Boolean Logic of course!

First things first, we need to understand basic operators in a search engine. These search engine operators are known as "Boolean". George Boole created the algebraic logic in the 1800's. He was an English mathematician, philosopher and logician. This algebraic logic, when applied to search engine queries, can yield specific results rather than searching for the words separately through all of the internet. In Boolean searching, an "and" operator between two words or other values (for example, "Deric AND Lostutter") means one is searching for documents containing both of the words or values, not just one of them. An "or" operator between two words or other values (for example, "Deric OR KYAnonymous") means one is searching for documents containing either of the words.

This is particularly helpful when searching for specific people, in specific areas. For instance we know that John Smith may live in or around Des Moines, Iowa. My first strategy would be to search for any social media accounts about him to see what he lists. To do that I would open a search engine such as Google, and type "John Smith" Des Moines, Iowa.

This search term would yield any results for Des Moines, and also any with the keyword "Iowa", in the search results. Quotations around the name means it is searching for that exact phrase, after all you don't want a bunch of documents about John Wall and Smith Forge Cider, you specified "John Smith".

Boolean also helps when searching for Social Media sites. Say you receive a strange email, or you are hired to find the identity behind an email. Providing that the email isn't a throwaway account and the person behind it isn't too careful, you can search with the specific quotation operator Bob@Bobgetsdoxed.com and anything associated with that email address will populate in your search results.

BASIC SEARCHING	EXAMPLES

Quotation marks
" "
Common Words Usually Ignored
+ or " "
to search them
	• Requires words to searched as a phrase, in the exact order you type them.
	`"working mothers"`
	`"affirmative action"`
	• Search `which versus that`.
	Only `versus` is searched on. `Which` and `that` are ignored.
	• To require common words to be searched:
	`+which versus +that`
	`"which versus that"`

Excluding -word -"phrase in quotes"	`"acute pancreatitis" diet -cat -dog -"pancreatic cancer"`

OR allows more than one term
OR
 
 	
`dogs OR cats`
allows pages with at least one of the terms
	• **OR** requires at least one of the terms joined by it to appear somewhere in the document, in any order.
	`"african americans" OR blacks`
	`ear OR nose OR throat`
	• The more words you enter connected by **OR**, the more documents you get. Broadens the search..
	• USES:
	o The **OR** operator is generally used to join similar, equivalent, or synonymous concepts.
	"global warming" OR "greenhouse effect"

AND (default)  `dogs AND cats` is the small overlap where both terms occur	• **AND** is the default and only needs to be typed if you are using other Boolean operators with ( ). `infopeople training` is logically the same as `infopeople and training` • The more words you enter connected by **AND**, the fewer documents you get. All your words will be searched on • USES: o The **AND** operator is generally used to join different kinds of concepts, different aspects of the question. o **"global warming" AND "sea level rise" AND california**

Tools to use for Doxing

- Google Search or any search engine of your choice (Remember Boolean!)
- Spokeo – offers reverse email lookup, phone lookup, address search, social media search, username search and more.(www.spokeo.com)
- SpyDialer – Until recently, offered a VoiceMail option where you could listen to the user's voicemail, who often said their name, which helped in verifying phone number. Offers name lookup, photo lookup. (www.spydialer.com)
- TheHarVester – Python program, available installed in Kali Linux distro - provides us information of about e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key server. Supports Google – emails, subdomains/hostnames
    - Google profiles – Employee names
    - Bing search – emails, subdomains/hostnames, virtual hosts
    - PGP servers – emails, subdomains/hostnames
    - LinkedIn – Employee names
    - Exalead – emails, subdomain/hostnames
    - New features:
    - Time delays between requests
    - XML results export
    - Search a domain in all sources
    - Virtual host verifier
- Whois searching – Reveals the registrar data behind the website if left unprotected, typically displaying the address and personal data of who made the website.
- Whitepages – a useful tool to verify address
- Beenverified or any other background check site
- Cain and Abel – Find IP behind XBOX-Live https://www.youtube.com/watch?v=e19D9E3e0b0

There are plenty more tools available on the internet, these are just a few to get you started. Get creative!

Social Engineering

From Wikipedia:

"**Social engineering**, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals"

How It Works

Social engineering exploits a flaw in the human behavioral system called "Cognitive Biases"

From Wikipedia

"Cognitive biases are tendencies to think in certain ways that can lead to systematic deviations from a standard of rationality or good judgment, and are often studied in psychology and behavioral economics."

The most common social engineering attacks happen over the phone. One can use, (at their own risk of breaking laws), the information gathered about the target during the recon phase, (Spokeo, social media monitoring, etc.), to call into an ISP or internet service provider, pretend to be a manager, perhaps from something like, Tier 3 support, and have the lower, Tier 1 support, lookup the address of the target assuming that we already have the IP. All this would take is confidence, an affirmative, official tone, sense of urgency, and 9 times out of 10, it works.

Other examples of social engineering include, but are not limited to;

- Pretending to be an exterminator, maintenance, tech support, or other official to gain access to areas civilians aren't allowed in.

- Walking into a building and posting false bulletins on company boards such as "Help Desk Number" has changed, thus giving the engineer passwords and ID credentials of employees.
- Pretexting: Creating a scenario by divulging information about the target found by prior research, such as birthday, address, last 4 of the social security number, or other identifying information. For example, calling into somewhere pretending to be target wanting to make account changes, or pretending to be someone with pre-conceived authority such as a insurance fraud agent to find out even more information such as account numbers.
- Diversion Theft: having packages that may contain company property delivered elsewhere by posing as a member of the company and speaking directly to the courier.
- Phishing : The art of "stealing" information about the user who clicks a link that is sent to them that could link to a false form that has the end user enter information about themselves, such as name, address, birthday, social security number, and more. This works because people typically only stare at the webpage without bothering to check the link in the address bar.
- Baiting: leaving a virus infected flashdrive or CD-ROM in a easy to see space such as table, elevator floor, or bathroom, in hopes that an employee will find the curiosity overwhelming, and insert it into their machine, thus infecting their computer revealing company data.
- Quid Pro Quo (Something for Something): The attacker calls random numbers pretending to be help desk support. Eventually someone ends up on the phone with a legitimate problem grateful for the help. The attacker then can instruct the victim to execute various commands and navigate to links to install malware on the system giving him access. Similar instances occur where employees (90% according to a 2003 I.T. survey) gave up passwords in an answer to a "survey" question for a cheap gift such as a pen.
- Tailgaiting: Bypassing RFID or other restricted gateways in a business by exploiting the common courtesy that someone will hold the door open for you if you are following them closely.
- Spoofing email addresses (making it appear the email is coming from a valid source)

Examples of Social Engineering in Popular Culture:

- In the movie *Identity Thief*, Melissa McCarthy used pretexting to get the name and other identifying information of Jason Bateman enabling her to steal his identity.
- In the film *Hackers*, the protagonist used pretexting when he asked a security guard for the telephone number to a TV station's modem while posing as an important executive.
- In Jeffrey Deaver's book *The Blue Nowhere*, social engineering to obtain confidential information is one of the methods used by the killer, Phate, to get close to his victims.
- In the movie *Die Hard 4.0*, Justin Long is seen pretexting that his father is dying from a heart attack to have an On-Star Assist representative start what will become a stolen car.
- In the movie *Sneakers*, one of the characters poses as a low level security guard's superior in order to convince him that a security breach is just a false alarm.
- In the movie *The Thomas Crown Affair*, one of the characters poses over the telephone as a museum guard's superior in order to move the guard away from his post.
- In the James Bond movie *Diamonds Are Forever*, Bond is seen gaining entry to the Whyte laboratory with a then-state-of-the-art card-access lock system by "tailgating". He merely waits for an employee to come to open the door, then posing himself as a rookie at the lab, fakes inserting a non-existent card while the door is unlocked for him by the employee.
- In the television show Rockford Files, The character Jim Rockford used pretexting often in his private investigation work.
- In the popular TV Show The Mentalist, protagonist Patrick Jane often uses pretexting to trick criminals into confessing to the crimes they committed.
- In the TV show Burn Notice, many characters are seen using social engineering; in Michael Westen's psych profile it is stated that he is very skilled in social engineering.
- In the TV show Psych, protagonist Shawn Spencer often uses pretexting to gain access to locations he would otherwise not be allowed into without police credentials.
- In the videogame Watch Dogs, protagonist Aiden Pearce states that he studied social engineering when growing up into a life of crime and uses social engineering tactics to manipulate other characters throughout the game to get the information he wants.

Doxing – Where to Look

Important Places to Look

It is important to realize this one simple fact. Everything you need to know to identify your target is more than likely already online, published at their own free will. This is what makes this practice completely and totally 100% legal. I will use myself as an example. When the FBI raided me in April of 2013, I explained to them the process of doxing someone, using myself as an example. I explained using reverse searches and Spokeo, I was able to find a safehouse that I lived in as a child, e-mail address included. The safehouse was an address that we lived at due to my mother being beaten repeatedly. The FBI agent stated, "Well, that just seems illegal." My response was "if it is, go arrest Spokeo and Whitepages, it was my own fault for putting out information so publicly."

Simply put, as shown in the graph in this tutorial, information is exponential in nature. We start off small, and one thing just grows to another, eventually we give all of our information to have access to popular social networking sites like Facebook.

So where do we start? We look in places like Facebook, LinkedIn, Google+, and just compile the information. Maybe Facebook isn't so locked down, and we expose our birthday, we expose our friends list which can tell our relatives. Hell, even Facebook has the option to name "who you are in a relationship with" and "relatives". From that information, we can then begin to build a family tree. Maybe your address isn't public yet, but your parents is, meaning I can reach out to them to get to you. I don't like what you have been doing, maybe you have been harassing someone, and maybe you have been all out rude and derogatory towards woman or a friend of mine. You listed your job online, you listed your relatives, now I can make your life hell with a

few simple screenshots

Dox Structure

Structure of Dox's should be as follows to make it in an easy to read format:

Target name:
Date of birth:
Phone Number:
Email addresses:
Address:
Workplaces:
Relatives:
Social Media Accounts:
Incriminating Evidence:

Doxing Tactics

Converting IP Addresses

The following sites can help you convert IP to physical addresses giving you a general location of the target.

- IPLocation: http://www.iplocation.net/
- IP2Location: http://www.ip2location.com/
- Convert Longitude and Latitude to Address: http://stevemorse.org/jcal/latlon.php

Pastebin.com

A popular site to upload documents to that requires no sign-up and allows the search of keywords such as name or usernames.

Reverse Image Search

When finding out information about a profile, they could have posted various photos in their Twitter feed, or timeline, that are also on other profiles they own. Reverse image search comes in handy in these scenarios. In order to utilize that, you can use these sites.

- https://www.tineye.com/
- https://www.imageraider.com/
- https://images.google.com/

How you can monetize doxing

Doxing can be monetized in several ways.

- Helping people track down long lost relatives
- Catching cheating spouses by exposing secret profiles
- Exposing and/or catching catfish accounts
- Finding names behind screennames harassing people
- Find out if a parent's child has any secret social media accounts
- Helping law enforcement catch career scam artists or other criminal

Conclusion

Doxing is an art, which has many different facets of the form. You can build your own style, your own routine as there is no "right way" to dox. The contents contained herein, are my methods. Tried and true, they have served me well over the years as I am sure they will serve you. I strongly recommend enrolling in my Ethical Hacking course, as these two things go hand in hand, and there are many tools, that require you to only click buttons, that can take advantage of the methods I have described today. Doxing is legal, up and until the point you access things like, credit card numbers, social security numbers, or anything privately stored in government databases. Use these skills wisely, and use them nobly. Thank you for your continued support. We are Anonymous. We do not forgive. We do not forget. Expect Us.

-Deric Lostutter
KYAnonymous
Opsec CyberSecurity Solutions
www.opsecLLC.com

http://www.facebook.com/realkyanonymous
http://www.twitter.com/dericlostutter