Doxing:
Dangers and Defenses

By Julia Moyer
Mentor: Ming Chow
Fall 2016

Table of Contents:

Abstract:

With the explosion of the Internet and social media came both great communication advantages, and vast privacy issues. Among the scariest for the everyday Internet user is doxing – the practice of making people's personal information publicly available where it used to be private or hard to access. This information can sometimes be gleaned from hacks and IP lookups, but is more often than not retrieved using everyday online tools such as search engines, social media profiles, and reverse phone lookups. Once an attacker has gained an individual's information, there is no limit to their malice. Techniques include cyber bullying and intimidation, public humiliation, fake sign ups for services, ransom requests, and most menacingly, stalking and child abduction. Though many of these attacks were possible before the age of the Internet, the web facilitates access to information that could have taken much more time and risk to gather in earlier days. Increased security settings are a must to help protect information posted to social media. Even more important than technological security advances is widely distributed literature about the advantages of using such security settings, as everyday web users are often painfully unaware of the consequences of open profiles. To take an even more extreme view, large social media outlets should take on the responsibility of defaulting all user profiles to maximum security.

Introduction:

Techopedia defines doxing (alternatively, doxxing), as "the process of retrieving, hacking and publishing other people's information such as names, addresses, phone numbers and credit card details".[1] While this definition covers many applications of doxing, to really understand the practice, one must additionally have an understanding of its common motivations and implications. It may be targeted at a particular individual, an organization, or a specific demographic (see "Known Cases" for more details on female gamer-specific attacks)[1], and may be prompted by curiosity, social activism, or (most typically) malicious intent, acquisition of power, and coercion[1]. Often, an attacker gains nothing material from the hack. Rather, the intent of the attack is to shame, humiliate, blackmail or take revenge on a victim.[3] An attacker is often motivated to dox someone whose online presence (including blogs, articles and social media comments, and posts) insults or offends them in some fashion.[4]

Doxing, whose name originated from the file extension ".doc"[1], is characterized by file tracing and sharing.[3] Most often, the information that attackers collect is publicly available on social media and phone lookup sites. However, the victim rarely expects or intends for these pieces of information, spread out at various locations around the internet, to be pieced together to form a full picture of their life, location, and identity. For example, in 2014, Garrett Bryant posted an innocuous relationship status change to his Facebook profile. Several friends commented on the post congratulating him, unintentionally revealing that Garrett's new partner was another male. Garret quickly deleted the post, afraid his Boy Scout leaders would find out about his sexuality, but the damage had been done. Due to tracing on social media, Garrett's sexuality was exposed and his chances at working at a Boy Scout camp were demolished.[3] This example goes to show that very minimal resources are needed for an impactful dox. The rest of this paper will explore other known cases of doxing, the methodologies successful doxers have used, and potential mitigation strategies the public should be aware of.

To the Community:

Though the formal name may be unfamiliar, doxing is an attack that almost everyone living in the twenty first century has heard stories of, read articles about, or even been victim to, regardless of their relationship to the tech world. Before I even had an inkling of interest in technology, I'd heard horror stories about cyber bullying and abduction via doxing practices. Doxing is not an attack that only governments, elite technology companies, and advanced hackers are affected by. Doxers are generally not targeting high-security information, but rather looking to cause personal and emotional damage. Doxing affects our neighbors, our friends, our children, and us. Think about it: how many people do you know that update any sort of social media profile? How many times have you sent a password or email address over a public network? How many emails have you sent to unknown recipients, or comments have you posted on a insecure blogging website? Any one of these actions has the potential to expose your emails, passwords, photos, IP address and other identifying information to doxers in a dangerous way. In the world where there is virtually no option to remain private, we must all be informed of the dangers that come with the powerful virtual tools we use everyday. The aim of this paper is to disperse basic knowledge of the types of attacks my readers are liable to fall victim to, and how to protect themselves from real, on- and offline danger and harassment.

Methodologies:

Doxing methodologies can range from very basic Internet searches, to more advanced hacks into private emails and social media outlets. This section will explore the tools and methodologies required for several different levels of attacks, as well the most common platforms for dispersing the acquired information.

Information Gathering and Tools

Most doxes begin with minimal and easily available information such as a username or a social media profile and require tools as simple and cheap as an anonymous email address, a search engine, and some social engineering skills.[5] From here, the attacker must gather as much basic information on his victim as possible. This generally includes information like email, home address, IP address, personal operating system, phone number, website, and photo.[5] Once in possession of this information, he can then progress to gathering more sensitive information, although sometimes the basic information is plenty to meet the attacker's needs.

There are several common methods and tools for acquiring the essential information about a victim. Since everyone's online presence is different, there is no fixed place for an attacker to start looking. A common start is examining at the victim's social media profiles, which can be found on search engines such as Pipl,[6] Spokeo[7] and Knowem[8] by linking a given name or username to connected accounts. A large amount of additional information can be gotten from social media pages, including location, family members, friends, and information about workplace. Using name and location, an attacker can utilize a site like whitepages.com[9] or 411.com[10] to search for the exact address of the victim.[11] If, instead of social media, an attack has access to the victim's email address, there are a number of straightforward ways he may attain the victim's IP address. On whatstherip.com[12], he may enter his own email, and select a link to send to the victim. When the link is clicked, the IP address will be sent directly to the attacker's email. IPs can also be obtained from any email that the victim has sent to the attacker, in the source file.[5] Using the IP on ipaddress.com[13], the attack may gain access to the victim's exact location, as well as operating system and

ISP. Finally, an attacker can upload his victim's photos to tineye.com[14] to see where else they are posted, or search their personal webpage on who.is[15] for additional personal details.

Public Platforms

In many cases, obtaining the victim's personal information is not enough. Although some attackers will use their newly acquired network of facts to silently stalk, or to steal from their victims, doxing is characterized by the posting of the victim's information on a public platform, such that the victim feels threatened, and the attacker's network also has access to the information. One commonly used site is PasteBin[16], which, though mostly used for sharing stories and ideas publicly, is notorious for its part in distributing stolen and illegitimate information.[17] Similar sites like 4chan and Reddit have also seen their fair shares of doxed information.

Known Cases:

As previously discussed, methods and motivations for doxing can vary widely across cases. In this section I present several well-documented cases to demonstrate several of the various forms that doxing can take.

The KKK:

Anonymous is an international hacking group, known for its activism in the political, social, religious and institutional realms. It is an open group, comprised of hackers all over the world, each working for the cause in which they most strongly believe. According to one ex-member, the only unifying goal is to fight oppression.[18] On November 5th, 2015, Anonymous leaked hundreds of names of alleged KKK members onto Pastebin (see Methodologies).[19] The Anonymous hackers were able to retrieve the names by accessing a Klan-controlled Twitter account. From there, they could view all information the account was privy too.[20] This dox was likely carried out via fairly simple tools such as network sniffers and password crackers. In this case, doxing was arguably used for good – namely, to encourage reform or remorse in the exposed members of hate group – but doxing, even when well intentioned, can still be ethically ambiguous. In 2014, a member of Anonymous doxed

a Ferguson police officer who he believed to be responsible for Michael Brown's death. As it turned out, he had it wrong. With one simple mistake, the officer's life was altered.[20]

Zoe Quinn:

In August 2014, Zoe Quinn's personal identifying details, including her name, home address, email, Twitter handle and phone numbers were posted to 4chan.[21] The gamer was forced to temporarily relocate, out of fear for her safety. The previous year Quinn had released a computer game called "Depression Quest," based off of (and in an attempt to cope with) her own struggles with depression. She immediately started receiving violent hate mail from other members of the gaming community who thought her release was too sad, too boring, and a disgrace to the gaming community, as it didn't follow the standard "rules" of computer games. The threats intensified after Quinn's ex- reported that she had had relations with a reporter who reviewed the game. While this turned out to be untrue, it launched a flood of tweets using the hashtag #gamergate to protest unfair game coverage in the media. Ironically, all attacks targeted Quinn rather than the reporter. In many ways, the Zoe Quinn case is a prototypical example of a malicious dox. The attacker's motivation was anger and hatred of a media that his victim had produced. His goal was to shame, scare and coerce her. His succeeded in opening the door for more members of the gaming community to attack and ridicule her. And, as is often the case with doxes – see the *KKK* section above – the attacker had a larger agenda; namely, to push women out of the gaming industry by putting them at risk for real, physical danger.[21]

Scarlett Johansson and other celebrities

Between November 2010 and October 2011, hacker Christopher Chaney gathered information on celebrities like Scarlett Johansson, Mila Kunis and Christina Aguilera[22] from their personal emails, including nude photos and private emails.[23] In a final release, he forwarded all information to two celebrity websites, which, in turn, made everything public. This attack is somewhat unique among doxes in that the perpetrator was identified and sentenced to time in court (10 years, in Chaney's case). As such, his methods were revealed and made public. After obtaining the celebrities emails (presumably through wiretaps and/or

network sniffing), he used the "Forgot your password?" link to answer each celebrity's security questions using publicly available information on the internet.[23]

Defenses:

Doxing's beauty (and its danger) is in its simplicity. An impactful attack does not require advanced code or any expensive tools. Intuitively, it seems that such a simple attack would require only a minimal defense. In some ways this is true, but in the reality of the world today, it is virtually impossible to stay off the radar of a skilled doxer. There are, however, many things both individuals and corporations can do to drastically reduce the probability of doxing attacks. This section will detail some of the steps that you can take, as well as what to do if the precautions fail and a doxing attack occurs.

Prevention

Trying to prevent a dox is like trying to prevent yourself from catching a cold: you can take all the necessary precautions, but still can't totally eliminate the chances, short of isolating yourself from society. You have likely lived many years of your life updating profiles, sending messages, and signing up for services. Even if you cancelled all accounts right now, there would likely still be enough information out there to leave you susceptible to an attack. However, simple changes can significantly reduce your chances of being doxed. One of the most important is to limit your privacy settings on all social media accounts – especially Facebook, as the site is one of the first that many attackers look at.[24] Although you may think that your profile is safe for strangers as long as you're not posting your email and address, doxers can get valuable information just from scanning your pictures and friend list. If an attacker was to obtain your email or username from another source, he could make an educated guess at your password security question using information he gained from your Facebook profile. Just like that, he controls your account.

A second important and very commonly overlooked prevention method is to use multiple emails to connect to various accounts.[24] Through sites like Pipl, attackers can search by email for connected accounts. This means that, if all your accounts use the same email

address, access to one profile may lead to access to many. Additionally, if the attacker has your email and has been able to obtain your password, he is likely to guess that many accounts use the same email/password combination. Do not let this happen! Simply changing around your email, username, and password combinations can do significant work towards deterring doxing attacks. The last simple step that everyone should take is to use the attacker's tools against him. With a simple search for your name, username and email on Pipl and the other search engines mentioned in the Methodologies section, you can track down your own most vulnerable information sources. After finding them, of course, you must remove or increase the security on them.

Before closing this section, I would additionally like to make several suggestions to corporations wishing to protect their employees and their businesses. It is essential, especially in at-risk fields like journalism and public safety, that new hires are able to undergo security training and are taught how to properly handle encrypted files. All employees should be directed to keep business and person emails separate.[4] In this way, there is a reduced likelihood of an attacker being able to connect personal and professional information from an employee. It also keeps company information safe from being exposed via an employee doxing attack.

Coping

Though taking the above steps is an excellent start to preventing a dox, it is possible that a determined attacker will still be able to hunt down the information he seeks. If this happens to you, you must know that it is not your fault. Victim blaming is common when it comes to doxes, as there is a widespread misconception that "staying away from the internet," or "not being too revealing" is enough to eliminate all chances of being doxed. As this paper has highlighted in numerous sections, this is simply not the case.

If you have been doxed, try to stay calm. Panic is a normal and instinctive reaction, but try to take time to assess the situation and its severity. Is the doxer someone you know? Have you felt threatened by this person in the past? Is the information posted on a public platform, or has it been sent only to you as a scare tactic? After considering these questions, if you feel threatened or afraid for your safety, do not hesitate to contact authorities. Make

sure to document the dox with screen shots and timestamps so that you may accurately report it and have the best chance of taking action against the doxer if you choose to do so.[25] Whether or not you choose to notify authorities, be sure to communicate the event to the people that will provide you with the best support network. However, try to refrain from posting anything about it on social media. This will 1) let the doxer know that he's gotten to you, and 2) potentially confirm the accuracy of the information that he has gathered.[25] Finally, it is sometimes a good idea to lessen your online presence until you feel that the threat has passed. Doing this is not conceding to the attacker – it is outsmarting him by avoiding taking his bait. The less attention is drawn to the dox, the less likely your information is to be picked up by another party.

Conclusions:

In part because it doesn't require a great amount of technical expertise or knowledge, doxing is one of the scariest security issues currently affecting the general population. What makes it doubly dangerous is that, rather than to gain something material for themselves, doxers often attack purely to emotionally abuse their victim or make an ideological point. Doxing can be difficult to predict and even harder to defend against. Though this paper has identified cases of doxing that are arguably ethical, such as the exposure of hundreds of members of the KKK, I believe that the practice itself is inherently harmful. When taken to extremes, it violates individuals' reasonable rights to Internet privacy, and is rarely carried out with non-malicious intentions. As we have seen, believing strongly in a particular cause is not ethical justification for doxing. Consider the gamers who felt so vehemently about the future of game development (and likely about female presence in the field) and drove Zoe Quinn into hiding at a friend's home. The fact that the Internet provides radical individuals with so many resources to harm others is undeniably scary. But luckily, there are several good measures to take to protect against such attackers. Restricting our online presences and being careful about the credentials we use to sign up for online services are good ways to start. As the Internet continues to grow and develop, we must all maintain our vigilance and do our best to alert others of the dangers that the Internet introduces.

References:

[1] @Techopedia. "What Is Doxing? - Definition from Techopedia." Techopedia.com. Accessed December 08, 2016. https://www.techopedia.com/definition/29025/doxing.

[2] Ramesh, Srikanth. "What Is Doxing and How It Is Done?" GoHacking. July 16, 2016. Accessed December 08, 2016. http://www.gohacking.com/what-is-doxing-and-how-it-is-done/.

[3] Leitsinger, Mir. "Boy Scouts Won't Hire Me for Summer Job Because I'm Gay, Teen Says." NBCNews.com. April 29, 2014. Accessed December 08, 2016. http://www.nbcnews.com/news/us-news/boy-scouts-wont-hire-me-summer-job-because-im-gay-n91731.

[4] Eveleth, Rose. "How to Deter Doxxing." Nieman Reports How to Deter Doxxing Comments. Accessed December 08, 2016. http://niemanreports.org/articles/how-to-deter-doxxing/.

[5] "How to Dox Anyone." Ctrlaltnarwhal. 2012. Accessed December 08, 2016. https://ctrlaltnarwhal.wordpress.com/2012/10/21/how-to-dox-anyone/.

[6] "The Most Comprehensive People Search on the Web." Pipl - People Search. Accessed December 08, 2016. https://pipl.com/.

[7] "Search People. Reunite." Spokeo. Accessed December 08, 2016. http://www.spokeo.com/.

[8] @knowem. "KnowEm Username Check for Social Networks, Domains and Trademarks." KnowEm Social Media Username Search. Accessed December 08, 2016. http://knowem.com/.

[9] "People and Public Records Search." Find People, Phone Numbers, Addresses & More | Whitepages. Accessed December 08, 2016. http://www.whitepages.com/.

[10] "Find Neighbors, Distant Relatives or Anyone in the Country." 411 - Free People Search | 411. Accessed December 08, 2016. http://www.411.com/.

[11] "How to Dox Anyone." WonderHowTo. Accessed December 08, 2016. http://null-byte.wonderhowto.com/how-to/dox-anyone-0160998/.

[12] "Instantly Find Someones IP Address." Instantly Find Someones IP Address. Accessed December 08, 2016. http://whatstheirip.com/.

[13] "What Is My IP Address? IP Address Tools and More." WhatIsMyIPAddress.com. Accessed December 08, 2016. http://whatismyipaddress.com/.

[14] "TinEye." TinEye Reverse Image Search. Accessed December 08, 2016. https://www.tineye.com/.

[15] "WHOIS Search, Domain Name, Website, and IP Tools - Who.is." WHOIS Search, Domain Name, Website, and IP Tools - Who.is. Accessed December 08, 2016. http://who.is/.

[16] "Pastebin.com - #1 Paste Tool since 2002!" Pastebin. Accessed December 08, 2016. http://pastebin.com/.

[17] "The Use of Pastebin for Sharing Stolen Data." Lenny Zeltser Content. March 16, 2015. Accessed December 08, 2016. https://zeltser.com/pastebin-used-for-sharing-stolen-data/.

[18] Sands, Geneva. "What to Know About the Worldwide Hacker Group 'Anonymous'" ABC News. March 19, 2016. Accessed December 08, 2016. http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302.

[19] Franceschi-Bicchierai, Lorenzo. "Anonymous Hackers Officially Dox Hundreds of Alleged KKK Members." Motherboard. November 5, 2015. Accessed December 08, 2016. http://motherboard.vice.com/read/anonymous-hackers-officially-dox-hundreds-of-alleged-kkk-members.

[20] Ohlheiser, Abby. “What you need to know about Anonymous’s big anti-KKK operation.”Washington Post. November 5, 2015. Accessed December 8, 2016. https://www.washingtonpost.com/news/the-intersect/wp/2015/11/05/what-you-need-to-know-about-anonymouss-big-anti-kkk-operation/?utm_term=.6f114df627c9.

[21] Parkin, Simon. "Zoe Quinn’s Depression Quest." The New Yorker. September 09, 2014. Accessed December 08, 2016. http://www.newyorker.com/tech/elements/zoe-quinns-depression-quest.

[22] "Johansson Hacker Gets 10 Years." The Daily Beast. 2012. Accessed December 08, 2016. http://www.thedailybeast.com/cheats/2012/12/18/johansson-hacker-gets-10-years.html.

[23] Winton, Richard. "Scarlett Johansson 'humiliated, Embarrassed' by Celebrity Hacker." Los Angeles Times. December 17, 2012. Accessed December 08, 2016. http://latimesblogs.latimes.com/lanow/2012/12/celebrity-hacker.html.

[24] Freeman, Allen. "Don't Get Doxed: 5 Steps to Protecting Your Private Information on the Web." WonderHowTo. 2012. Accessed December 08, 2016. http://null-

byte.wonderhowto.com/news/dont-get-doxed-5-steps-protecting-your-private-information-web-0133806/.

[25] "So You've Been Doxed: A Guide to Best Practices." Crash Override Network. 2015. Accessed December 08, 2016. https://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices.