**Hacktivism and the threats it can create for Data Integrity**

**By Jacob Letterman**

**Abstract**

Hacktivism is the unauthorized access of computer files for political or social reasons. This paper is discussing the threats that can come from said hacktivism. This paper will specifically talk about the threats that face data integrity now, in the near future, and later in the future. These are predictions, but they are all based on trends and research that have been conducted looking into how data integrity is affected by hacktivism. These questions were created due to the, at the time of writing, invasion of Ukraine by Russia, and how hacktivist groups have released several hundred classified Russian government documents in wake of said invasion. Due to research, it was found that many threats that were once conceived as something that will never happen or might happen in the far future, will happen at a faster rate than we could have ever imagined.

**Introduction**

What is Hacktivism? Hacktivism, as defined by the Oxford dictionary, states that it is the “unauthorized access of computer files or networks to further social or political ends.”. This is a relatively new term, with it really only being applied after the early 2000’s, with groups such as Anonymous or Wikileaks. As stated before, the reasons for this type of activism are generally put into 2 categories, social or political ends. The political side has been prevalent at the time of writing with the Russian invasion of Ukraine, with many documents of the Russian government being released in the wake of said invasion. The social side is often mixed with the political side, as many of the goals are the same, but they should be noted as separate channels of hacktivism as they are often used by different groups for different reasons, hence them being two different reasons for hacktivism.

This topic, to me at least, is very interesting as its connotations with social informatics can be quite impactful. Recently with the Russian invasion of Ukraine, and Wikileaks with the Iran and Iraq wars. This got me thinking about how this type of hacking can impact our daily lives, would it be for the better or for the worse, or more specifically, how bad of a double-edged sword could this be. Many problems involve data theft or how data integrity is loss when faced with these types of cyber-attacks, but it can become much worse than just those examples. I started to think about what would happen to data integrity as a whole, not just with personal data, as that would most likely be destroyed if attacks were to continue, also destroying anonymity on the internet that we value so much when online.

Data integrity is something that many people either don’t talk about, or don’t want to talk about. What I mean is that people don’t want to think about the effects of losing their data, their personal data, and sometimes, even their business due to a hacktivist trying to prove their justice to the world and hurting innocent people on the way. The way that it is heading, these problems will become more and more prevalent. This paper is split up into 3 sections. The first section will go into detail about the threats that data integrity face now, the second section will go into detail about threats that may happen in the near future, and the third section will go into detail about threats that, if they do happen, will not happen for a long time.

**Threats: Now**

The type of threats that we face now with data integrity, will have an effect on if the effects of the future threats come to pass or not. The main threat that we may face now is data theft.

Data theft is the main thing that hacktivist do in order to continue their goals, it is typically described as “stealing data, intellectual property, or other information via ransomware or other malicious attacks.” (CrowdStrike, 2021). Data theft is something that many are worried about, and yet, they have no idea how bad it can truly be. In this digital age, everyone is connected online, whether they want to or not, and with our data being on there, hackers can try and steal our money or identities if they feel it is for their justice.

The next threat is based off of the last one. Money is something that allows us to do literally almost anything in the world, and that is more prominent today than it has ever been. So, when a hacktivist has your account, they could use your hard-earned funds to either pay for something that they want or give that money to people who they believe deserves it. They could also cause disruption of service attacks that can cause people who want to use your service, not able to use it. Another type of attack is an attack via exploiting bank systems or the federal reserve, both of which would cause catastrophic damage to our entire banking, making all of us lose money due to a hacker wanting to show that something is corrupt or unjust or they want to prove themselves better than someone/something else.

This prediction is really for businesses affected by hacktivism. Businesses need business and customers need service from said business, and if the business cannot provide that service, the customer will go to somewhere else. A hacker will typically do this via a DDoS attack, denial of service attack, which is when a system is shut down and prevents customers from accessing the site. This may seem like it would never happen to you and the services you use, and you might be right, but don’t forget that many hacktivists don’t do this because of financial gain, they do it for attention, the more people that know about them, the better for them.

If the trends for hacktivism continue, the threats that might be near, will come to happen.

**Threats: Near**

The threats that we face in the near future have a chance to happen, but really only have a small chance depending on if the previous predictions happen, but if they do, then here is what will happen. The biggest thing that can happen is almost, if not entire loss of data integrity. Data Integrity is important not just for us, but for everyone that is involved on the internet. It may seem like it only talks about safety of data, but DI is important as it “is the overall accuracy, completeness, and consistency of data.” (Talend, 2020). Everything we read, watch, and look at falls under this, and if that’s gone, we lose any sense of reputable sources as we wouldn’t know what data is actually truthful, and data that was made up to try and make people believe that others agree with their opinion.

With it being the most important thing for internet users, the total loss of anonymity on the web would be disastrous for many. This may not seem like a huge loss, as many people already use their real name when on Facebook or Twitter, but it is much more than just your name. Your address, work address, phone number, and email address can be tied to one of your accounts, and that is even the least of what can happen. Just having that isn’t what makes it dangerous to you, it’s what the hacker can do with it that makes it dangerous. Doxing is when someone’s personal information is leaked on the internet, causing them to get swatted, when people get a fake threat about someone committing a great crime, or once again, have someone’s identity is leaked, causing them to get it stolen and used for any purpose the thief wants to use it for.

Of course, these predictions are based on trends that are slowly increasing, but if they were to come true, this could mean that Data Privacy in of itself could become completely lost.

**Threats: Later**

At this point in the paper, speculation is really the only way to think about the future of data integrity and data privacy. Don’t think of these predictions as based on nothing, they are based trends and other cases that help with painting a picture of what could happen in the future, a complete loss of data privacy. Data privacy is how we are able to keep our data anonymous from anyone who would like to know who it belongs to. This is how we can be truly anonymous online, as our data connects back to us, though for some that is harder due to uses of VPNs and other technologies. Imagine you click on a website, and you accept the cookies that it gives you and you sign up for a membership. That data is able to be tracked back to you if someone were able to access the companies’ files. These breaches are becoming more and more common, with bigger and bigger companies, as that creates the most publicity, meaning more people know about them. Privacy is how we can feel safe knowing that we can be anonymous to a bunch of strangers online, but if that were to go away, then hacker would have an easy time of getting our data and then selling to the highest bidder.

**Conclusion**

In conclusion, there are many threats that can happen to us if hacktivism were to increase, such as with lose of service for businesses or complete loss of data privacy, we would have threats that had nearly no chance of happening, actually coming true and coming faster than we would have ever would have imagined them coming. Thankfully, there are some things in place now that help with protecting people from hacktivism. Two-factor authentication is one of the best ways to protect your data integrity, as it shows if someone does try to get into your accounts and allows you to protect yourself from said hacker. Though it may feel like it is a losing game trying to protect your data integrity, there are thankfully ways to protect yourself from threats that are about to come or ones that have yet to come.

**References**

CrowdStrike. (2021, May 6). *What is hacktivism? why organizations should care: Crowdstrike*. crowdstrike.com. Retrieved April 14, 2022, from https://www.crowdstrike.com/cybersecurity-101/hacktivism/#:~:text=Being%20the%20victim%20of%20a,and%20privacy%20of%20private%20citizens.

Sorell, T. (2015, September 22). *Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous*. Academic.oup.com. Retrieved April 14, 2022, from https://academic.oup.com/jhrp/article/7/3/391/2412155

UNODC. (2019, June). *Cybercrime module 14 key issues: Hacktivism*. Cybercrime Module 14 Key Issues: Hacktivism. Retrieved April 14, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/hacktivism.html

Kerry, C. F. (2018, July 12). *Why protecting privacy is a losing game today-and how to change the game*. brookings.edu. Retrieved May 2, 2022, from https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

Talend (2020). *What is Data Integrity and Why is it important?* Retrieved May 4, 2022, from https://www.talend.com/resources/what-is-data-integrity/