Assessing Software Vulnerabilities on the Black Market

Kaleb Alstott

CIT 485- Advanced Cybersecurity

Dr. Awad Mussa

Fall 2022

Introduction

The term “black market” was found and dates to the year of “June 1927 in a statement about the influence of organized crime in the Teamsters union” (Just a Moment. . ., n.d.). The black market refers to an area of economic activity where the buying and selling of goods and services is conducted illegally. In today’s day and age, we are surrounded by the latest and greatest technology that is advancing at a tremendous rate. We find ourselves in the period of the Information Age. A digital age in which information can be process and transmitted within seconds. Today we must worry about possible cyberattacks and cybercrimes that are being conducted attacking our data and security rights. Software vulnerabilities are at an all-time high, “66,000 valid vulnerabilities this year - over 20% more than 2020 - with hacker-powered pen tests seeing a 264% increase in reported vulnerabilities.” (Software Vulnerabilities Increase by 20% in 2021 | HackerOne, 2021). With the increase in software vulnerabilities, we are in great danger, due to the availability of the black market where information can be currently bought, traded, and exchanged for financial rewards we must from a legal market or stop these actions or by possible preventing these exploits by machine learning techniques and monitoring. These vulnerabilities that hackers can buy and exploit onto companies is causing an economic and social crisis. Through intensive research there is an overall common goal of this topic in which we do know and understand that in this field, there needs to be a consistent study due to the dynamic changing filed of cybersecurity. Another important topic that has been found through the cybersecurity research by others, is what we now understand the black-market vulnerabilities in which the lifecycle of a vulnerability has a direct correlation to the vulnerability market. This refers to how long a vulnerability lifecycle last is directly respondent to the vulnerability market and if these vulnerabilities have been found or discovered yet. We can also conclude that through our research, Radianti and Gonzalez, offer a preliminary model of the vulnerability black market, we see the black market is continuously growing if there is no form of legal transaction market or proper disclosure policy implemented. One of the research gaps found in this study is needing proof of data of transaction in legal and illegal markets to form a proper conclusion on if legal markets will stop or reduce the illegal trade of software vulnerabilities on illegal markets. The second research gap found in this study is if machine learning capabilities can both be effective and perform correctly as intended, according to Younis and Malaiya and their model of *Using Software Structure to Predict Vulnerability Exploitation Potential*. This is done by taking machine learning techniques and predict whether a given vulnerability is likely to be exploitable or not. This is because of the new metric that can be used as an earlier indictor of vulnerability exploitation based on software structure properties, and black-market monitoring showing a 20% more effective strategy than those currently enforced according to findings in Allodi et al. (2013). In this research I have conducted, I’ve limited our scholarly articles to only the most recent information from the last two decades. I’ve chosen this most recent information due to the dynamic changing field in cybersecurity. When analyzing and reviewing these scholarly articles it was important to find information on current or possible legal markets that prioritized their legitimacy, attractiveness, and easy dealing with software vulnerabilities for rewards. As well as with the research of possibly implementing a safer form of protection against these software vulnerabilities such as using machine learning to understand patterns, vulnerability types, monitoring systems, and more to protect against any ambition of exploits being used from the black market to harm others. This is to show that if a possible legal market does not follow through with the results, we are anticipating that we have another idea or a backup plan to implement decreasing the number of software vulnerabilities exploited from the black market by predicting them through machine learning. With an illegal market that is continuously growing and transmitting software vulnerabilities to hurt companies or individuals economically and socially, there is a call of action to form not just a legal market but a market that is able to properly disclose software vulnerabilities quickly and effectively by following policy and machine learning capabilities.

At first, I would like to bring acknowledgement to software vulnerabilities and the black-market correlation by explaining what factors effect the emergence and growth of this illegal market. Followed by the lifecycle and possible correlations that software vulnerabilities have in the black market. Secondly, I would like to bring a solution of a federal legal market for software vulnerabilities to be properly disclosed with the intended policy. This section will also touch on what legal markets or possible legal market options have been presented and are implemented today. Lastly, I would like to bring your attention to what if we cannot conclude on a legal market that is both effective and reliable enough to change the direction of the black market? As well as limit the transaction of software vulnerabilities on the black market. This solution would come in a form of defense and protection with machine learning techniques that would be able to indicate vulnerability exploitation earlier, as well as techniques to predict whether a given vulnerability is likely to be exploitable or not.

Software Vulnerabilities and Black-Market Correlation

To understand the correlation between software vulnerabilities and the black market we must first know what a software vulnerability is. A software vulnerability is a “security flaw, glitch, or weakness found in software code that could be exploited by an attacker (threat source)” (Software Vulnerability - Glossary | CSRC, n.d.). This weakness in the software can be used to exploit privilege access controls, download malicious content, possibly missing data encryption, and much worse.

The term “black market” is a market that is usually illegal transactions of goods and services in which take place at prices higher than a legal maximum. In every market there is always going to be your buyers and sellers. In our case of software vulnerabilities on the black market we have black hat hackers who typically work underground and are anonymous. A black hat hacker is anyone that goes against and violates computer security for their own personal profit. These black hat hackers can be both our buyers and sellers. The black market can be very profitable, hackers and malicious actors can secretly buy, sell, and trade these vulnerabilities online at an alarming rate at which we cannot currently stop. What makes these software vulnerability transactions so attractive to black hat hackers and others, is due to the prices in the evolving black market. Which may be higher than what legitimate companies would pay for at first, till they realize how dangerous this vulnerability is to them and will tend to pay more for it. The main reason for hackers to search for these software vulnerabilities is to obtain higher opportunity for financial achievement through successful exploitation. Recently however these vulnerabilities are now being sold to whoever the highest bidder might be despite the damage it may cause (Algarni, 2014). We know that the black market is active due to the findings of, “a large fraction of the discoverers are from outside of the software development organizations, and that their key motivation is a monetary reward” (Algarni, 2014). From Algarni, we see that there is a large amount of software vulnerabilities being found outside the software development, meaning this leads us with the concern of increased zero-day exploits. Zero-day exploits are, “a computer vulnerability that is being actively practiced before knowledge of the exploit becomes public information." (Radianti, J., & Gonzalez, J. J., 2007, p.1). In both research articles of Algani and Radianti, Gonzalez, there is a strong proven correlation between the increase in zero-day exploits and the emergence and growth of the black market. We can prove the correlation by Radianti, J., & Gonzalez, J. J., stating, the black-market emergence and growth and the knowledge of hackers getting to these software vulnerabilities first, before the companies and public, we have seen an increased number of zero-day exploits (2007). With these studies being seven years apart it shows that there has been an importance in understanding that the black market has been accusable of these zero-day exploit increases. Due to this increase we can see how companies and software developers are scrambling to find these vulnerabilities before they happen or as soon as possible, understanding how important it is to patch these exploits. With the basic terminology and background information needed to understand what a software vulnerability is and how the black market works we can take a deeper dive into why it is important to understanding the lifecycle and relationship, software vulnerabilities have on the black market.

A vulnerability lifecycle is intended to allow organizations to identify computer system security weaknesses such as prioritizing assets, assess, report, remediate the weaknesses, and ensure that the vulnerability has been eliminated. A vulnerability lifecycle can start on a zero-day exploit or can be a current on ongoing situation that the software developers are trying to patch. The relationship that the vulnerability lifecycle is a direct coloration to the vulnerability market. The vulnerability market lifecycle is when once a vulnerability is found typically by a black hat hacker the vulnerability then enters the black market where the price can fluctuate depending on the severity, time of discovery, application/software, if the vulnerability has been patched, and of course type of vulnerability found. Both lifecycles depend on each other. This is important to understand due to the research gap in the legal market and how software vulnerabilities would have to work and be properly priced depending on these lifecycle's circumstances. Through my research I have found two scholarly articles that state that there is a strong correlation between the vulnerability lifecycle and the vulnerability market. In our first research article by Radianti, Rich and Gonzalez, we see an early statement of how these lifecycles might be dependent on each other, "Our initial examination of data indicates that these forums have a lifecycle and behaviors that support their need for both visibility and invisibility." (2009). The examination that these researchers found was a piece of information about the vulnerability and market lifecycle in which it depends on visibility, which correlates to if the vulnerability has been found, known about, or patched by the company. Thirteen years later in the research from Algarni he states, "Therefore, studying these markets with actual data and examining the relationship between vulnerability markets and the vulnerability lifecycle, theoretically, and statistically, is considered to be strong evidence that the vulnerability lifecycle depends on vulnerability markets. (2022)." The dataset used to identify this relationship between software vulnerabilities and market vulnerability lifecycle was a report on vulnerabilities for Mozilla Firefox and Google Chrome that were collected by Finifter et al. for the period 2009 to 2012, who analyzed cost-effective mechanisms for finding security vulnerabilities and had experts review the information for both browsers. Alagani, here confirms through his research that there is indeed a direct correlation between the vulnerability lifecycle and the vulnerability market. This means that with today's knowledge of how vulnerabilities work on an illegal market we can further advance our research gap into how a vulnerability lifecycle would look on a legal market and what would that lifecycle look like in comparison to the illegal market. It is important to note that knowing how the legal market and vulnerabilities work and the lifecycle will help us in our future research of creating a legal market that benefits form these lifecycles on both ends of the buyer and seller, as well as creating a proper responsible disclosure policy to ensure the correct actions are taken on these exploits.

<u>Ideas Of a Legal Market</u>

The idea of a legal market in which not just software vulnerabilities can be accessed, bought, sold, and traded on properly is not a new idea by any means. Within the past decade we have started to see a rise in companies trying to start some form of a legal market. Companies offer an incentive if there are any vulnerabilities reported to them that are unknown, for an exchange for financial reward. As stated, before by Algani, this is one of the main incentives from the seller, although we don't have any data statistically, we assume this is the case on why hackers trade on the black market (2014). These rewards programs that companies are holding not only benefit both the seller and buyer but also help improve our technology and understanding in a proper disclosed form. Through Algani early research on a legal market for software vulnerabilities, he was able to string together an example of this market that the software developers' companies are offering. Here is an example of what exact price would be paid depending on the attack type (zero-day exploit) and the developers of the product.

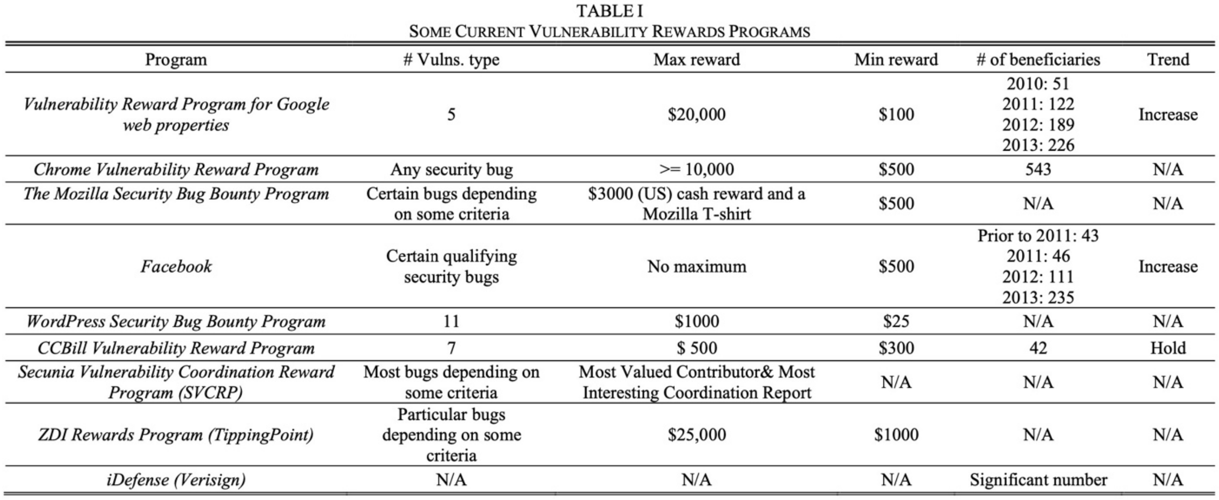

TABLE I
SOME CURRENT VULNERABILITY REWARDS PROGRAMS

Program	# Vulns. type	Max reward	Min reward	# of beneficiaries	Trend
Vulnerability Reward Program for Google web properties	5	$20,000	$100	2010: 51 2011: 122 2012: 189 2013: 226	Increase
Chrome Vulnerability Reward Program	Any security bug	>= 10,000	$500	543	N/A
The Mozilla Security Bug Bounty Program	Certain bugs depending on some criteria	$3000 (US) cash reward and a Mozilla T-shirt	$500	N/A	N/A
Facebook	Certain qualifying security bugs	No maximum	$500	Prior to 2011: 43 2011: 46 2012: 111 2013: 235	Increase
WordPress Security Bug Bounty Program	11	$1000	$25	N/A	N/A
CCBill Vulnerability Reward Program	7	$ 500	$300	42	Hold
Secunia Vulnerability Coordination Reward Program (SVCRP)	Most bugs depending on some criteria	Most Valued Contributor& Most Interesting Coordination Report	N/A	N/A	N/A
ZDI Rewards Program (TippingPoint)	Particular bugs depending on some criteria	$25,000	$1000	N/A	N/A
iDefense (Verisign)	N/A	N/A	N/A	Significant number	N/A

(2014) Software vulnerability markets: Discoverers and buyers. *International Journal of Computer and Information Engineering*, *8*(3), 480-490.

Although this rewards program is from this decade and not within the past five years, we are able to see the trend of a lot of companies to take on this program in hope of paying for a software vulnerability rather than paying the expenses and damages form one instead. This brings us to our research gap in the legal market which is why haven't we had a federal legal market for software vulnerability's to be properly transaction on and in between companies and other hackers. Through multiple research articles we have found two common denominators that have a strong coloration of why these markets haven't yet emerged in our economic system today. Research from Algarni in two separate papers and years, as well as Younis and Malaiya, state that due to the "dynamically changing field, studies such as this need to be repeated in order to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society", as well as "the need to collect data about the transactions in the regulated and the unregulated markets so that the processes can be modeled accurately"(2016/2022) (2014). What this means is that due to the ever-dynamic changing field of vulnerabilities and the market it is difficult to find trends, patterns, or observations that would help us further define our legal market with such type of reasonable rewards. Following the same idea of rewards and incentives for a legal market we find another research gap in this study stating that we lack heavily on statistical data of transaction on both types of legal and illegal markets. This can be difficult for us to form a legal market due to not knowing what the supply, demand, and price of vulnerabilities are to regulate a beneficial legal market with proper responsible policy disclosure. With this research gap there has been some other research articles that have taken a deeper dive to try to further bridge together the gap of the legal market. Algarni in his 2016 research, states three main steps to further understand forming a legal market that will benefits both sides. These three further steps that we need to take our, the need to create new vulnerability markets that are suitable for the different types of vulnerability discoverers, our markets should be legitimate, attractive, and easy to deal with so they are a good income source for both sellers and buyers, and lastly studying the rewards buyers give to sellers should be reasonable, depending on supply and demand and other commercial market concepts. Algani has a strong relationship connection to his earlier research as well as Younis and Malaiya, due to the understanding in what is stopping us from forming a legal market is the correct transactions, understandings of wants and needs, supply and demand, and a proper way of disclosing the vulnerability. Without having a firm statistical data of transaction on legal and illegal markets it is quite difficult to properly price and create a sustainable market without knowing trends and cycles in which we have yet to discover in a legal market. Although we have further knowledge and correlation to vulnerabilities lifecycles on an illegal market.

Understanding the research gap between the legal market and software vulnerabilities, and what separates us from the goals of a legal market are important to understand. These gaps in our research are the lack of statistical data in the legal and illegal markets that are not simulations, and the actual study on if these vulnerabilities have any type of pattern, or observation to further understand what type of software vulnerabilities are more attractive to black hat hackers compared to others that may by bought and sold on the markets. Further understanding what types of vulnerabilities, transactions, and reward incentives that are attractive, reliable, and easy to use will help us further close in on the research gap of a legal market and how to properly implement the wants and needs for both parties. Although in this research the legal market seems like the most economical and social pleasing answer that would benefit, some researchers have drawn some conclusions and theories on what would happen if a legal market were offered. In our first research article we are dealing with quantitative data from a dynamic simulation in which a concept model captures an abstract example of parallel legal and illicit markets. The researchers Radianti, Rich and Gonzalez, constructed their simulation model into four categories, the first scenario (Current) represents the absence of a legal market for overtly compensating hackers for their work. A second scenario (Legal Market) assumes activation of the legal market. A third scenario (Manifest) represents manifested through attacks or extortion threats. The others through reports to vendors, or postings on web sites, presumably with more information about how the problem was identified. Finally, a fourth scenario (Consumer) in which is referencing the consumer exposure to these vulnerabilities in these markets (2009). The results from these findings state that the illicit markets end up producing an increase in our software quality and accelerated patching along with the speed of which we must do this. Secondly, the process by which transitions from black to white markets develop and the resultant effects on overall software quality. Lastly, the vulnerability discovery is accelerated which also becomes necessary to speed the development of patches for these flaws. The key take aways to note from this simulation model is that illegal markets end up producing an increase in our software quality, patching speed, and lastly that if we do switch to a legal market that our overall software quality will be effected due to the transition in the market.

Although Radianti, Rich and Gonzalez produce a valid assumption with our software quality, and patching speed I find this a weak relationship since this is coming from a simulation and not real statistical data. We must take this conclusion with a grain of salt because we would need real data to confirm that these decreases in our systems would happen over time with the shift to a legal market. Although we can predict that our software quality might decrease and our patching speed decreasing, there is a stronger concern in the legal and illegal market. Researchers, Radianti and Gonzalez, state that with their dynamics system model showing the growth of the vulnerability black market, this simulation showed by having a legitimate market to which these vulnerabilities can be properly disclosed and by having a financial reward there is a shrink in the black market (2007, January). Although with this simulation there shows a mediate relationship by using this simulation and projecting the growth of the black market but what this study didn't take into effect and what we need statistical data, on is if the "hackers might sell the information to both parties: vendors and criminals. Our model so far neglects this issue and only considers the options of selling vulnerabilities to the vendors or selling them to malicious agents" (Radianti & Gonzalez, 2007). I find this a strong correlation since not many researchers at all have proposed the idea of what if hackers go to both parties to sell. I find this an extreme acknowledgement in this research gap that we need to understand what if they do sell to both markets. There needs to be a simulation that considers both markets being active with equivalent rewards and satisfaction. This would be a missing puzzle piece till we move on to the bigger and main research gap of "the need to collect data about the transactions in the regulated and the unregulated markets so that the processes can be modeled accurately" (Younis & Malaiya, 2014). With a stronger relationship to understanding the illegal market and legal market and what may come from these changes we are faced with another problem of what if our legal market fails? What if our market does shrink the black market but the black market is still active with vulnerabilities? In our next section we will cover how machine learning may help us protect and defend from these vulnerabilities and what is stopping us from implementing these actions.

Machine Learning Defenses

One of the many defense techniques talked about by researches to prevent and stop these software vulnerability attacks is the idea of adapting to a machine learning technique that can predict, indicate, and monitor software vulnerabilities on the illegal market. "Machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy." (Education, 2022). With machine learning becoming more frequently adapted into the cybersecurity field we see researchers starting to implement strategies, ideas, and theories about how machine learning can help protect against software vulnerabilities. To implement any type of machine learning techniques we must find a pattern in attacks, type of attacks, the cost and deficit of these attacks, and more. Researcher Algarni proposes the idea to build a stronger approach for identifying key factors contributing to the breach cost as well as assessing the impact of these breaches to allow for the correct resources, time, and efforts it takes in achieving the required security level you or your company desire (2016). Algarni has identified the most prolific vulnerability discoverers throughout the past decade and examined their motivation and methods, and have produced a quantitative data, computational model for estimating the costs and probabilities of data breaches for a given organization. With the statistically accurate data of the most prolific vulnerabilities past the decade as well as a structural model Alagani has concluded in his research that there is a strong relationship to starting a possible machine learning technique to warn about software vulnerabilities. His model concluded that it could scale an economical proportional data breach probability, that is able to properly allow for optimal investments and implementations to increase your security. I found that this was a building block for other researchers, and it showed with being able to predict an economical breach and what it would cost a company including financial and time management point of views. By further predicating cyber-attacks and vulnerabilities we find a very strong correlation to machine learning techniques with this being one of them. Another steppingstone in the field of machine learning to protect against software vulnerabilities of the black market is the idea of monitoring the black market. In research from Younis and Malaiya, their goal was to conduct a new metric that can be used for earlier detection and as an indicator, as well as a developed model that uses machine learning to predict rather a vulnerability is likely to be exploited or not (2014). Through Support Vector Machines (SVMs), they were able to produce a model based on machine learning techniques that uses the proposed metric as feature to predict the risk of vulnerability exploitation. This model was based off research models of using measurement-based approaches, model-based approaches, test-based approaches, and analysis-based approaches. With these approaches Younis and Malaiya, were able to construct the proper model with a strong correlation of statistical data that then were able to conclude that this software vulnerability monitoring system and new matric can be used as an earlier indictor of vulnerability exploitation based on software structure properties. This model also concluded that it could help decision makers prioritize their actions objectively based on function structure features. Through this research we can see that the idea of machine learning can be an adequate idea with successful results in properly identifying software vulnerabilities that could be possible on the black market. The theory of adapting machine learning techniques can also be adapted with black market monitoring. Research from Allodi et al. aims to understand the quantitative assessment of the risks coming from the market, as well as reducing overall attacks against users and companies (2013). The methods he used in this article range from the WINE-DB, EKITS, NVD, and CVSS score. The research in the article proposes, the numerous cyber-attack types that were recorded by WINE-DB and EKITS dataset from the black market, as well as their score on the CVSS. Showing that software vulnerabilities are being traded on the black market as well as the severity of these vulnerabilities. Second, using CVSS and EKITS as proxies for the risk of the vulnerability, as well as weighted average value of risk, concludes that patching strategies based on black market observations can be much more effective than those based on the traditional CVSS score by average of 20% (2013). This is because of the new metric that can be used as an earlier indictor of vulnerability exploitation based on software structure properties.

The idea of a new scoring system for vulnerabilities, vulnerability exploitation based on software structure properties, and the monitoring of the black market, can be properly implemented. Although there can be an implementation of these learning techniques, the same research gap is presented here as it was from the legal market research. Which is Algarni in two separate papers and years, as well as Younis and Malaiya, state the strong correlation of a "dynamically changing field, studies such as this need to be repeated in order to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society"2016/2022) (2014). What we are missing form these models and theories of machine learning techniques to spot and detect these software vulnerabilities is the overall effectiveness of the model as well as the overall performance of this model. Although researchers can clarify that this model can do what they attend there needs to be further research and testing to ensure the overall effectiveness and performance is sustainable enough to release to the public and companies. Even though there is no statistical data on how effect this system would be, I could imagine we would want this machine learning technique to be able to at least be able detect eighty plus percent of software vulnerabilities before they are exploited or before they can reach the illegal market. Now this is ideally what I could predict, there is no statistical data relaying any goals set out by these researchers but with this topic I would feel comfortable enough to release to the public and companies ensuring the effectiveness and efficiently in this solution. Till there is further research and confirmation done on machine learning techniques and how effective they may be to fight the battle against software vulnerabilities on the black market, we are left with the proposal of still learning and adapting to the ever-changing dynamic field of cyber-attacks and software vulnerabilities. As well as still trying to provide statical data in fields of legal and illegal markets to ensure the correct effectiveness, and efficiently of these defensives for the public and software companies.

Conclusion

To conclude the research gap of assessing software vulnerabilities on the black market, I have taken eight research articles of the most significance over the past decade to grasp an understanding at where we stand today with these vulnerabilities on the black market. Through my research we can conclude that we have found a strong correlation between the vulnerability lifecycle and the lifecycle of the illegal market. We can also conclude through our research that the strong correlation between the emergence and growth of the black market has caused a rise in the zero-day exploits that companies are suffering from today. There have been researchers that have offered up ideas and theories about a legal market and possible machine learning techniques in defense of these software vulnerability exploits. Although we have seen a shift towards a legal market already with companies taking on the model of offering financial rewards for vulnerabilities found in their software considering the still active black market. These models have encouraged a deeper understanding in what that we need to create a new vulnerability market that are suitable for the different types of vulnerability discoverers, the markets should be legitimate, attractive, and easy to deal with, so they are a good income source for both sellers and buyers. Lastly, studying the rewards buyers give to sellers should be reasonable, depending on supply and demand and other commercial market concepts. Looking into a legal market we have identified that there is pros and cons to implementing this type of market. Although this seems like the easiest safest options there is some speculation that draw concerns for having a legal market. There is statistical data stating that with a legal market the information being transaction on the black market does decrease but through simulations it shows a decrease in our software security, and parching rates as well. Although with a legal market we do lack a lot of real-life statistical data that represents the markets transactions the idea of a legal market is still in the top running for solving the issue of software vulnerabilities on the black market. If the idea and theory of a legal market never come to be there is another idea in the works of stopping these software vulnerabilities on the black market, and that is machine learning techniques such as monitoring and a new scoring system to rank vulnerability threats. With the new metric that can be used for earlier detection and as an indicator, as well as a developed model that uses machine learning to predict rather a vulnerability is likely to be exploited or not, along with the black-market monitoring concluding that patching strategies based on black market observations can be much more effective than those based on the traditional CVSS score by average of 20% (Allodi et al.,2013). We are left with the research gap of sufficient, reliable, effective statical data that can provide in both fields of legal and illegal markets. To ensure the correct effectiveness, and efficiently of these defensives for the public and software companies.Taking in these considerations and analyzing other research articles, I have made me drawn my conclusion in this research gap. Following the research from Algarni in two separate papers and years, as well as Younis and Malaiya, state that due to the "dynamically changing field, studies such as this need to be repeated in order to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society", as well as "the need to collect data about the transactions in the regulated and the unregulated markets so that the processes can be modeled accurately"(2016/2022) (2014). Our biggest research gap is providing actual evidence that is up to date with transactions on both legal and illegal markets as well understanding that in this field our data and content is changing daily and to keep up, we need extensive research with statistical data. This can be challenging though because as stated before it can be extremely difficult to find and track this evidence due to the privacy and limited interactions in the black market that take place in private chats and transactions between the buyer and seller. To conclude, there needs to be further research on both legal and illegal market transactions, as well as conducting a relevant study on the dynamic changing field to conclude any patterns, attack types, particular users, and most of all an analytic comparison between studies showing any type of similarities between the two markets. Finally, one thing I would like to note and bring attention to is the idea of having both the legal and illegal markets running. Through all the research only one article brough this to my attention and I would heavily consider to doing more research into what would happen if hackers sold on both markets compared to one or the other.

Reference Page

Algarni, A. M. (2014, February 3). *Software Vulnerability Markets: Discoverers and Buyers*. Zenodo. https://zenodo.org/record/1091516

Algarni, A. M. (2016). *Quantitative economics of security: software vulnerabilities and data breaches* (Doctoral dissertation, Colorado State University).

Algarni, A. M. (2022). The Historical Relationship between the Software Vulnerability Lifecycle and Vulnerability Markets: Security and Economic Risks. *Computers*, *11*(9), 137. https://doi.org/10.3390/computers11090137

Allodi, L., Woohyun Shim, & Massacci, F. (2013). Quantitative Assessment of Risk Reduction with Cybercrime Black Market Monitoring. *2013 IEEE Security and Privacy Workshops*. https://doi.org/10.1109/spw.2013.16

Education, I. C. (2022, July 6). *Machine Learning*. https://www.ibm.com/cloud/learn/machine-learning

Just a moment. . . (n.d.). https://www.encyclopedia.com/social-sciences-and-law/law/crime-and-law-enforcement/black-market

Radianti, J., & Gonzalez, J. J. (2007, July). A preliminary model of the vulnerability black market. In *25th International System Dynamics Conference at Boston, USA*.

Radianti, J., & Gonzalez, J. (2007). Understanding Hidden Information Security Threats: The Vulnerability Black Market. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. https://doi.org/10.1109/hicss.2007.583

Software Vulnerabilities Increase by 20% in 2021 | HackerOne. (2021, December 8). https://www.hackerone.com/press-release/software-vulnerabilities-increase-20-2021

Software Vulnerability - Glossary | CSRC. (n.d.). https://csrc.nist.gov/glossary/term/software_vulnerability

Vulnerability Black Markets: Empirical Evidence and Scenario Simulation. (2009). *2009 42nd Hawaii International Conference on System Sciences*. https://doi.org/10.1109/hicss.2009.504

Younis, A. A., & Malaiya, Y. K. (2014). Using Software Structure to Predict Vulnerability Exploitation Potential. *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion*. https://doi.org/10.1109/sere-c.2014.17