**Annotated Bibliography:**

**Assessing Software Vulnerabilities on the Black Market**

**CIT 485- Advanced Cybersecurity**

**Kaleb Alstott**

**Fall 2022**

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

With the slow steady increase in software vulnerabilities being sold and purchased for negative impacts on the black market, this work tries to establish what factors effect the emergence and growth of the black-market vulnerabilities. In this work the author contributes to multiple models that show unintended consequences of a policy intending to mitigate the software vulnerability problems. These models were based off a simulation that consisted of four main assumptions for the behavior of the system over time in the market. These four systems were the base run, full disclosure, a legal market, and lastly a risky environment. These models confirm that the vulnerability black market may not grow as fast as what is expected. Or the market could possible even be contained if the legal system can effectively create a situation where hackers will have higher risk of conducting cybercrimes.

This work does a great job of presenting valuable data and statistical analysis on a simulation of software vulnerabilities under different assumptions. This article lacks on the real statistical data of the software vulnerabilities available on the black markets, as well as validation on the data to show extensive research on the real-world problem. Although this article does a great job of explaining and demonstrating what the black market is and why software vulnerabilities are so critical along with what it means to being sold on this site. There is also a lack of policy to try and fix this situation or bring possible solutions to this problem such as a policy for responsible disclosure of these vulnerabilities.

Algarni, A. M., & Malaiya, Y. K. (2014). Software vulnerability markets: Discoverers and buyers. *International Journal of Computer and Information Engineering*, *8*(3), 480-490.

With the idea of an ideal market for software vulnerabilities to be regulated, this article goes in depth into the actual vulnerability market, both the regulated and unregulated, to gain a better concept of where and why this information is being sold. Through rigorous research this article has provided the most prolific vulnerabilities over the past decade to understand the motivation, methods, and the overall risk it has on society today. The model demonstrated in this article gives an idea of all seven markets that software vulnerabilities can be bought and sold on. The results of this work shows that majority of the vulnerabilities found are outside of the software developers company, and the motivation behind these attacks are mostly due to money. This work also showed that in regulated markets such as reward programs, the software vulnerabilities are disclosed in a proper and responsible way compared to the unregulated markets.

With the in-depth look at all seven markets that software vulnerabilities can be sold and bought on, as well as the detailed firsthand experience obtained, the data in this article is sufficient and up to date. With the market continuously growing and new software vulnerabilities found every day, it would be ideal to do this type of research monthly to start to see patterns or even the frequency of software vulnerability types. The article also touches on all markets and possible values given in each market depending on the vulnerability type. With this there should be another detailed research into the markets, to confirm possible values and changes that have occurred during this time to ensure solid proof of the data found along with the reliability.

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

As software security becomes a growing concern for individuals and companies, this article investigates the vulnerability regulated markets of Chrome and Firefox. As well as the correlation between vulnerability markets and the vulnerability lifecycle, and how these contributions may put people and companies at a security and economic risk. We come to find out that the main motivation behind these vulnerabilities sold on the market is a financial reward and satisfaction. This making the contribution to believing that if vulnerability markets can be controlled, the vulnerability lifecycle will be reduced/ possibly eliminated, along with any other associated risks. The research model used in this was an available dataset of reported vulnerabilities for Mozilla Firefox and Google Chrome, form the time of 2009-2012, that analyzed cost effective tools for finding security vulnerabilities. The findings form the article state that there is a strong correlation between the vulnerability lifecycle depending on the vulnerability markets.

With the strong use of actual data and not a simulation in this article, we are given a strong statistical analysis. What this article lacks however is the proper regulation and policy implementation of a proper regulated market. This correlation of the regulated market would demonstrate greater evidence needed to support the claim of vulnerability lifecycle depending on the vulnerability markets. Another supporting factor needed for this research is an updated data set of regulated markets from this decade to compare possible vulnerability lifecycles and market comparisons.

L. Allodi, W. Shim and F. Massacci, "Quantitative Assessment of Risk Reduction with Cybercrime Black Market Monitoring," 2013 IEEE Security and Privacy Workshops, 2013, pp. 165-172, doi: 10.1109/SPW.2013.16.

With the knowledge about software vulnerability and attack tools being traded in the black-market to harm others, this article aims to understand the quantitative assessment of the risks coming from the market. As well as reducing overall attacks against users and companies. The methods 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%.

With the use of real data and not a simulation we are given an excellent contribution of what attacks are being traded on the market as well as what risk they bring to others. Although this research is valid, there needs to be deeper research into tracking the vulnerabilities traded on the black market and if there is a direct correlation to possible attacks that were excecated by using the methods of WINE-DB and EKITS. Lastly, a demonstration on how to proxy the black market as a company or individual and what it would take for a single person or team to understand this concept and implement it where need be.

A. A. Younis and Y. K. Malaiya, "Using Software Structure to Predict Vulnerability Exploitation Potential," 2014 IEEE Eighth International Conference on Software Security and Reliability-Companion, 2014, pp. 13-18, doi: 10.1109/SERE-C.2014.17.

Due to the recent study of new software vulnerabilities being discovered and having a significant impact on cyberattacks, as well as the implementation of the time gap between the vulnerability public disclosure and the release of an automated exploit getting smaller draws a concern for many societies safety. In this research the proposition, of 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. These findings are based off the research models of using measurement-based approaches, model-based approaches, test-based approaches, and analysis-based approaches. This model demonstrated in this research can help prioritize decision making actions based on machine learning techniques, as well as having an earlier indication on exploitability content by using the new metric demonstrated.

Although the research conducted demonstrates a new metric to scale exploits and vulnerabilities there is no measure of success or effectiveness of using the propositions proposed in this article.

Without the use of real data identifying that the new metric scale and machine learning techniques are producing the earlier detection rate that is proposed all we have is a very well-constructed model that gives us an idea of how this may work.

J. Radianti, E. Rich and J. J. Gonzalez, "Vulnerability Black Markets: Empirical Evidence and Scenario Simulation," *2009 42nd Hawaii International Conference on System Sciences*, 2009, pp. 1-10, doi: 10.1109/HICSS.2009.504.

With vulnerability black markets having a naturel unknown and hidden transactions sparks the question of if these markets produce the creation of media and security companies and if so, how are they effected in comparison to a legal market. This article also desires to introduce a simulation model that produces how vulnerability discoveries possibly can be placed in a duel legal black-market concept. Through the research conducted we find that there is a possibility of these markets existing to help and create these security and media companies due to the lifecycle and behaviors of the vulnerabilities. Through the methodology of simulation, we look at both legal and illicit markets. We find that illicit markets end up producing an increase in our software quality and accelerated patching along with the speed of which we must do this.

Although this article produces a great statistical analysis of a duel legal black market, we lack the necessity of the relational value between creations of media and security companies to these black markets. There is little evidence and lack of knowledge in the first part of this article describing the situation between security companies and media correlation to the black market.

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

With security breaches on the rise yearly this study searches 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. The article gives us actual data representation of the significant factors minus the redundant factors to merge a quantitative model of data breach costs and probability. This model can scale an economical proportional data breach probability, that is able to properly allow for optimal investments and implementations to increase your security. When looking at the reason why data breaches occur this article leans on who is behind the actual vulnerability finders, and what motivates them.

This article, although is filled with loads of real data that provide a great depth and understanding of the scores used in the quantitative model and how the model is used properly, I find this article overexplaining and going into too much background information. I find that this author hit on not just one main point but what felt like four or five points throughout the whole article. This article tries to cover too much in the aspect of what factors goes into a data breach and can be challenging to follow all topics.

Radianti, J., & Gonzalez, J. J. (2007, January). Understanding hidden information security threats: The vulnerability black market. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156c-156c). IEEE.

Due to the rise of the black market and illegal trade of vulnerabilities, there has been an effort to try and establish a legitimate legal market. This study aims to see exactly if the legal market helps reduce the trading of vulnerabilities on the black market. From this article we can see the come abouts as well as the dangerous growth of the black market. 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. By using simulation software Vensim, we can simulate what a legal market would do as well as the opportunities of what the market may be instore in the future. Although other parties play a significant role in shortening the number of vulnerabilities on the black market, the speed at which these other parties can find solutions is lesser than the speed of the hackers.

Although the study did a great job of presenting simulated data from both the legal and illegal market, what this study lacks is the simulation for both the markets. The what if the hacker sells data to both the legal and illegal market what happens? This research also lacks in the depth of the black-market expansion if it is a possibility as well as what exploits and vulnerabilities could happen with the transition of many companies heading into the legal market.