Counter-Ransomware Project

Kinnick Fox

Bellevue University – DSC680

10/11/2023

In this paper, I will be writing about the [Title], its execution, and an analysis of the visualizations.

Business Problem

Businesses around the globe contend with the threat of cyber attack on a daily basis. Ransomware is a particularly nasty attack that is capable of halting all operations that rely on data within a compromised device. The goal of this project is to identify key features that make an organization the target of ransomware as well as to speculate the best cybersecurity solution for organizations with those features.

Background

Ransomware is a malware that leads to a highly disruptive cyber-attack that denies the user of a key system or data. “Ransomware has quickly become the most prominent and visible type of malware” (Check Point, n.d.). It was created to target large organizations and individual users alike. Ransomware, like all malware, does not simply manifest within a system or server, it must penetrate defenses and gain complete control of the target.

Data Explanation

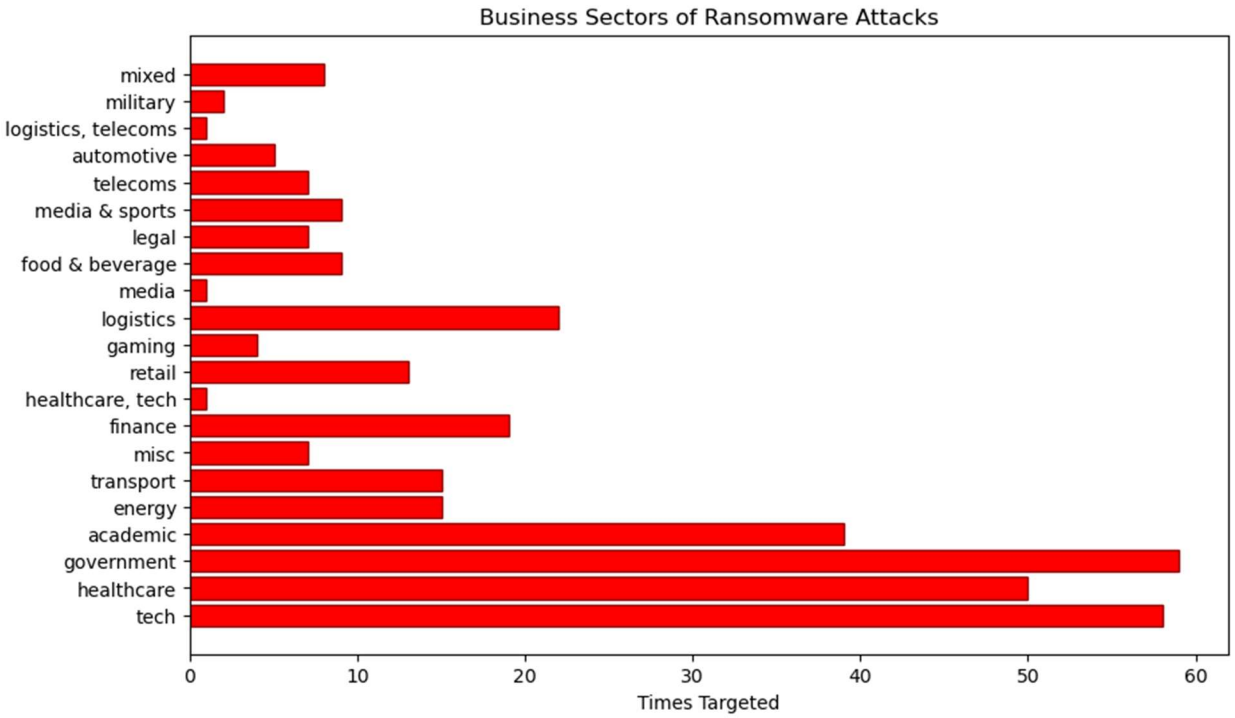
Kaggle will supply the dataset for this project. Joakim Arvidsson’s Ransomware Attacks found at https://www.kaggle.com/datasets/joebeachcapital/ransomware-attacks contains target’s business sector, organization size, ransom size, location, revenue, and ransomware used features that may be useful in analysis. The dataset is missing large

quantities of data but should still contain enough to gleam some form of insight. The dataset is also quite messy and will need some cleaning before it will be usable.

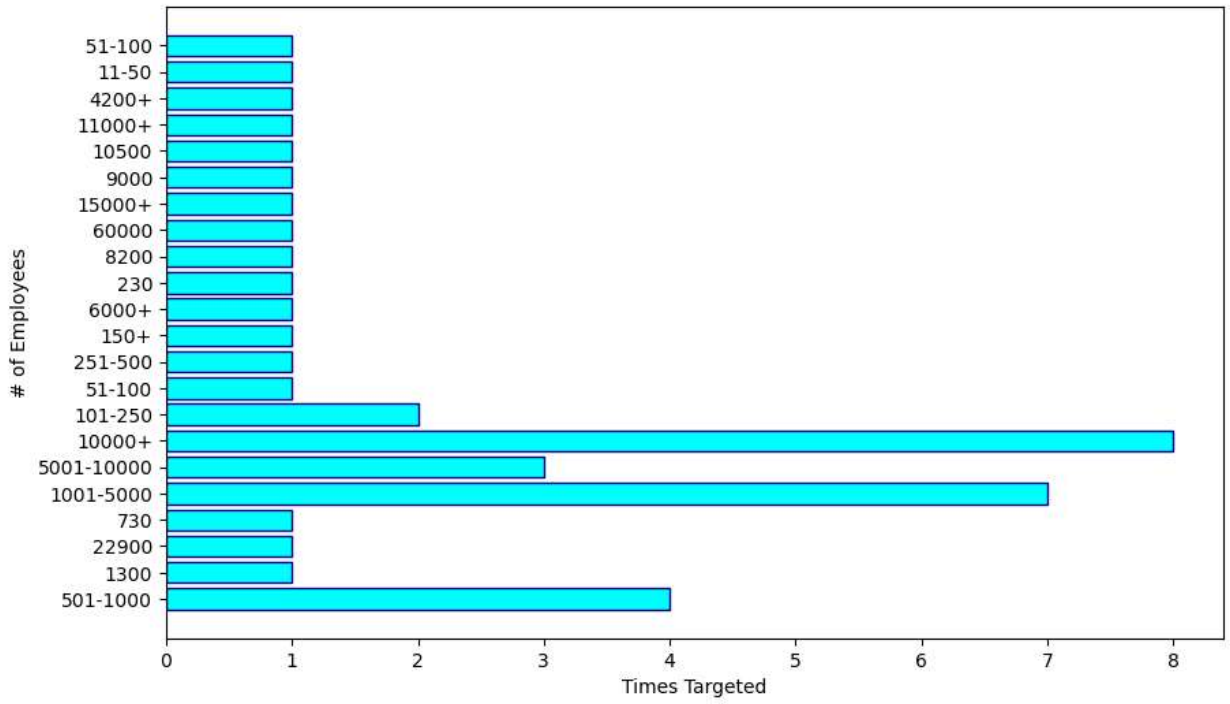
Method

Due to the type of quantity of data available, a modeling solution was not beneficial for this project. Instead, I will be deriving insights from various plots and figures that this dataset can produce. Remaining unbiased to results will be key in finding objective insights.

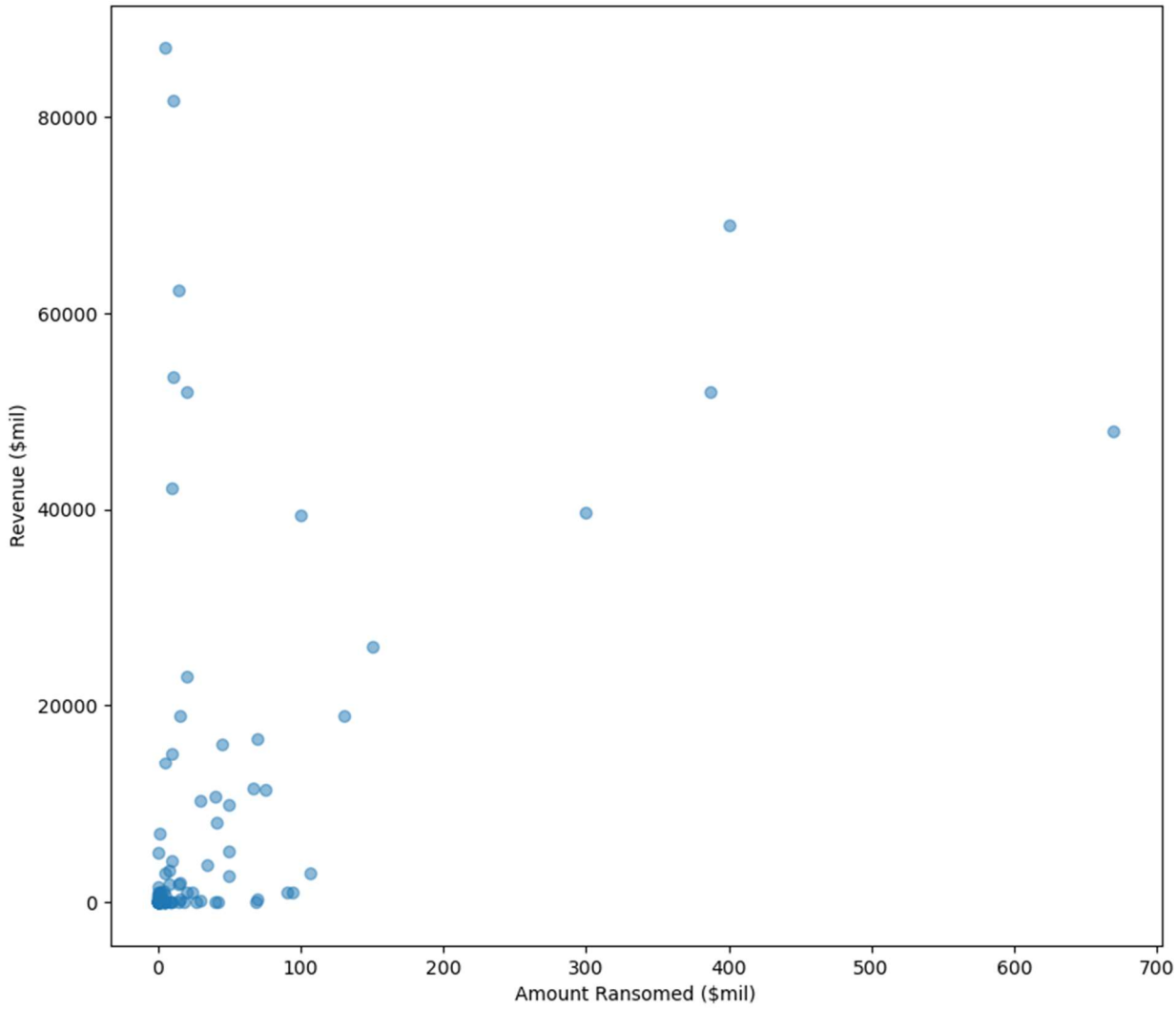
Analysis



This visualization shows that the most commonly targeted business sectors are academic, government, healthcare, and tech.



This visualization shows how size of business, in regard to the number of employees working for that business, relates to the amount of ransomware attacks received. It appears that the more employees that work for a company (the larger it is) increases the chance of ransomware attack.



This scatterplot shows the relationship between a company's revenue and the amount they were ransomed for. I was expecting a more substantial trendline to show a linear relationship between these features. One does exits somewhat but not enough to be conclusive in any way. The majority of ransom demands appear to be below $30 million, many below $10 million targeting both small companies and huge billion-dollar companies alike.

Conclusion

Analysis shows that larger companies within the academic, government, healthcare, and tech business sectors are more at risk of ransomware attack. The demanded ransom will most likely fall below $30 million.

Assumptions

The major assumption that is being made for this project is that the available data is representative of the missing data. If this was not the case then any insights gained from this dataset would be inaccurate.

Limitations

As mentioned previously, this project was unable to be successfully modeled so all insights and analysis are speculative. That said, bias was avoided in analysis of the visualizations.

Challenges

The main challenge for this project was cleaning of the dataset. Data was prepared per visualization in order to preserve useful data that may not have necessary data for every visualization used. Another challenge with this type of data is that many features are not usually made public. It is up to an organization whether or not to publicize the fact that they were the target of a cyber-attack, which will often lead to scrutiny in regards to the cybersecurity practices of that organization. This can be seen in the chosen dataset as most of the columns are ~60% “unknown” variables. The impact of this will not be known until analysis begins.

Future Uses

The intended use of these results are to inform companies if they are of greater risk of ransomware as well as how damaging a ransomware attack can be. Sharing these results and/or expanding this research to other modes of attack could be even more beneficial to businesses.

Recommendations

As a BS holder in cybersecurity, I would recommend that any company, no matter how large, regularly backup data on an offline device. This will deny the attacker their goal of cutting the entity off from the desire data. Attackers tend to leverage social engineering to gain access to a system so additional training for employees on how to spot suspicious activity would also be beneficial for companies that this project found to be more likely to be targeted by a ransomware attack.

Implementation Plan

Presenting these finding to a company under the pretense of cybersecurity training would most likely be the best use of these results. Additionally, as stated earlier, expanding to other attacks and possible vulnerabilities would be beneficial for companies.

Ethical Assessment

Providing companies with information that can protect them and their customers form cyber-attack is very ethical. Although, it is important not to give businesses false expectations or take advantage of a business that becomes panicked when made aware of possible vulnerabilities.

References

ARVIDSSON, J. (2023, August). *Ransomware Attacks*. Retrieved from Kaggle: https://www.kaggle.com/datasets/joebeachcapital/ransomware-attacks/code

Check Point. (n.d.). *What is Ransomware?* Retrieved from Check Point: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware