Predicting and visualising ATM attacks

Bouke Regnerus and Raoul Fasel
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente
7500 AE Enschede, The Netherlands

I. Introduction

ATM attacks and fraud continue to make headlines. The compromise of ATMs is a very lucrative criminal business. ATMs typically exist as physical contact points of the banking infrastructure that are exposed to public sight. This makes ATMs a very accessible target for exploitation, vulnerable to a large variety of attack scenarios. The European ATM Security Team report that the amount of ATM attacks both physical- and logical attacks only increase [1], therefore securing ATMs but also predicting ATM attacks are more important then ever.

This paper describes the process of both visualising ATM attacks and predicting cases where ATM attacks could occur. The main focus of this of this research is the exploration of using tools provided in the DM- and DPV topics provided in the Data Science course. Furthermore other tools such as the Python machine learning library Scikit-learn and JavaScript data visualisation library D3.js will be used.

A. The Dataset

Provided for this project is a dataset from the European TREsPASS project [2] that was developed in collaboration with Spanish banks. The dataset contains information of 723 ATMs, attacks on those ATMs and the information about those attacks. In more detail, the dataset provides: geographical details about ATMs (such as latitude and longitude coordinates, distance to a highway), demographic details (such as per capita income, population density, median population age), logging details of the attacks per ATM, the profile of the involved attacker, the information on how much amount was recovered and when did recovery event took place.

For this research the most important features of the dataset are both the geographical- and demographical features. Those features can be used for both visualising attacks and predicting attacks using a classifier with those features as an input.

B. Research Questions

With the DataScience DM and DPV topics in mind this lead to the following research questions:

> How can a dataset containing geographical- and demographical features of ATM attacks be predicted and visualised?

This question is answered with the support of the following questions:

- Which factors contribute most to attack frequency and attacker success?
- How can factors that contribute to attack frequency and attacker success be plotted geographically?
- How can ATM attacks be predicted using a Naive Bayes classifier?

II. Method

To give an accurate answer the above mentioned research questions multiple different tasks have to be conducted.

Lorem Ipsum

A. Application of Topic DPV

Lorem Ipsum

B. Application of Topic DM

Lorem Ipsum

III. Results

Lorem Ipsum

IV. Conclusion and Discussion

Lorem Ipsum

References

[1] European ATM Crime Report Archives — European ATM Security Team, European ATM Security Team. [Online]. Available: https://www.european-atm-security.eu/tag/european-atm-crime-report/. [Accessed: 13-Apr-2017]

[2] The TREsPASS Project. [Online]. Available: https://www.trespass-project.eu. [Accessed: 13-Apr-2017]