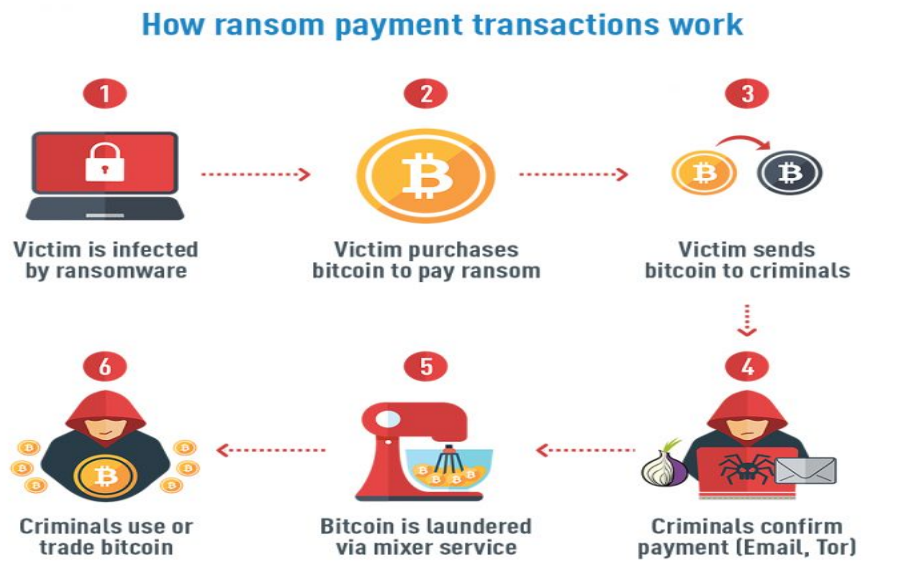
Predicting Ransomware patterns in a BitCoin graph

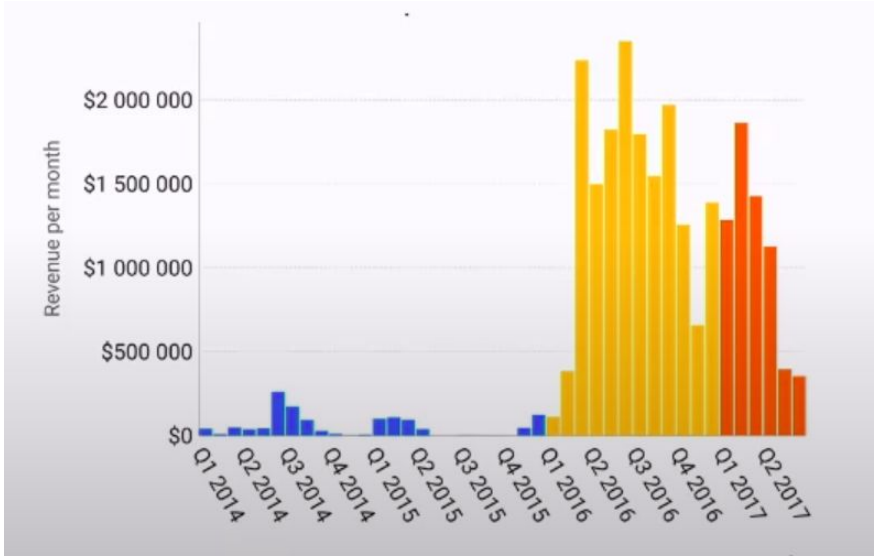
Shannon R. Serrao

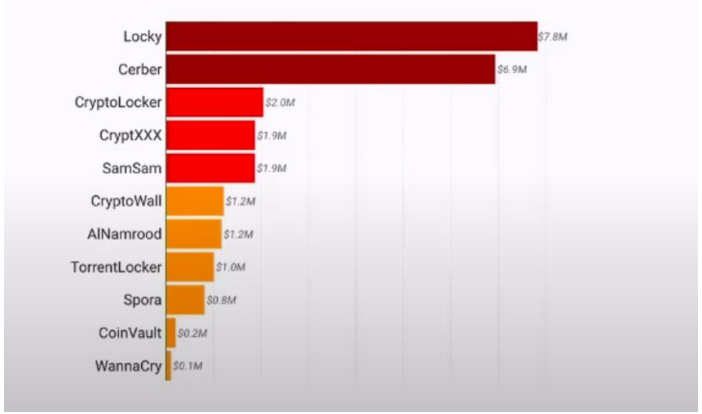
Seasonal variation of Ransomware families

Github repo

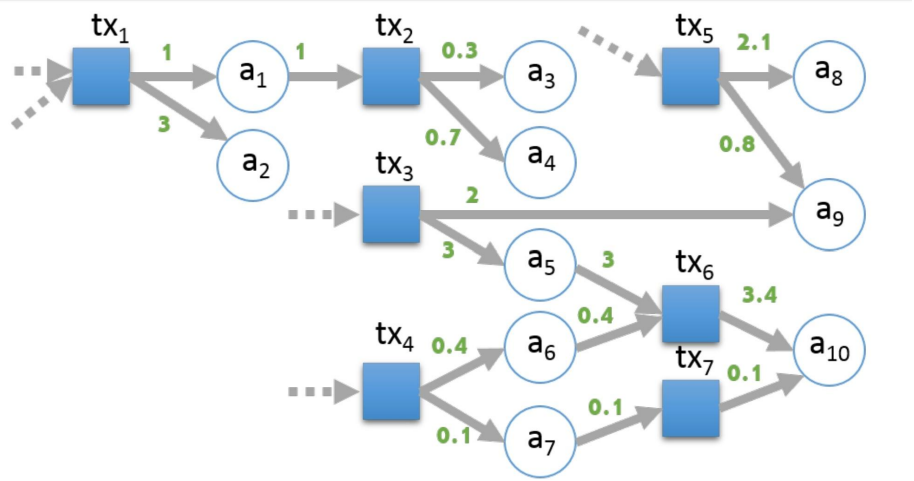
What is Ransomware ?







Tracking Ransomware on a Blockchain



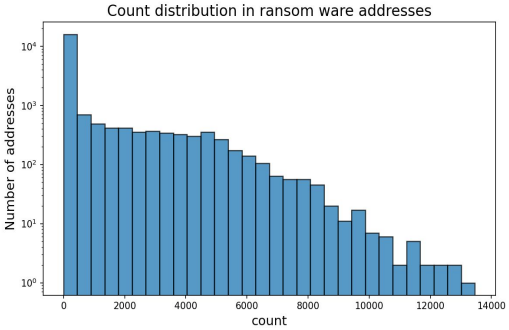
Features

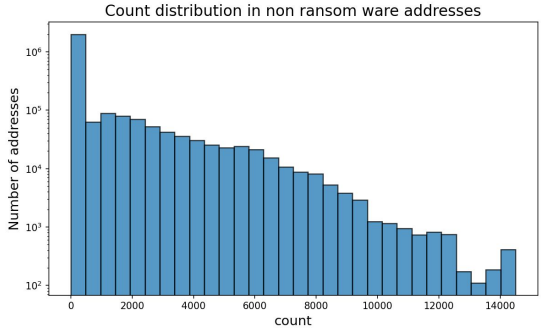
- Count
- Length
- Income
- Count
- Weight
- Neighbors

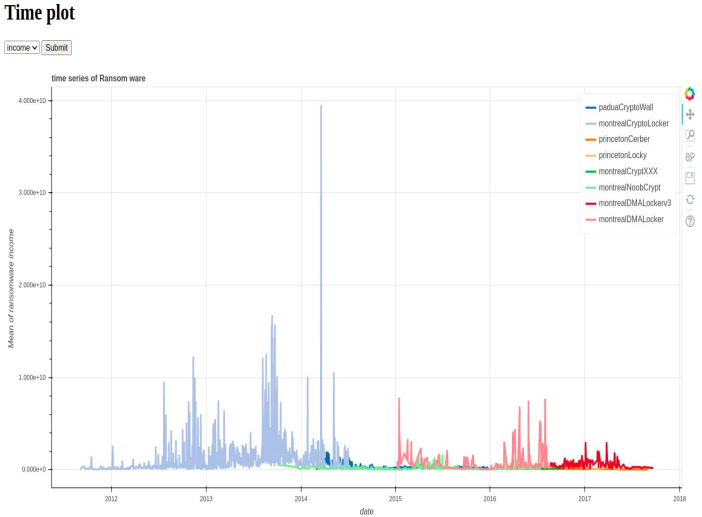
Dynamic activity of Ransomware transactions

Heroku app: [Seasonal variation of Ransomware families]

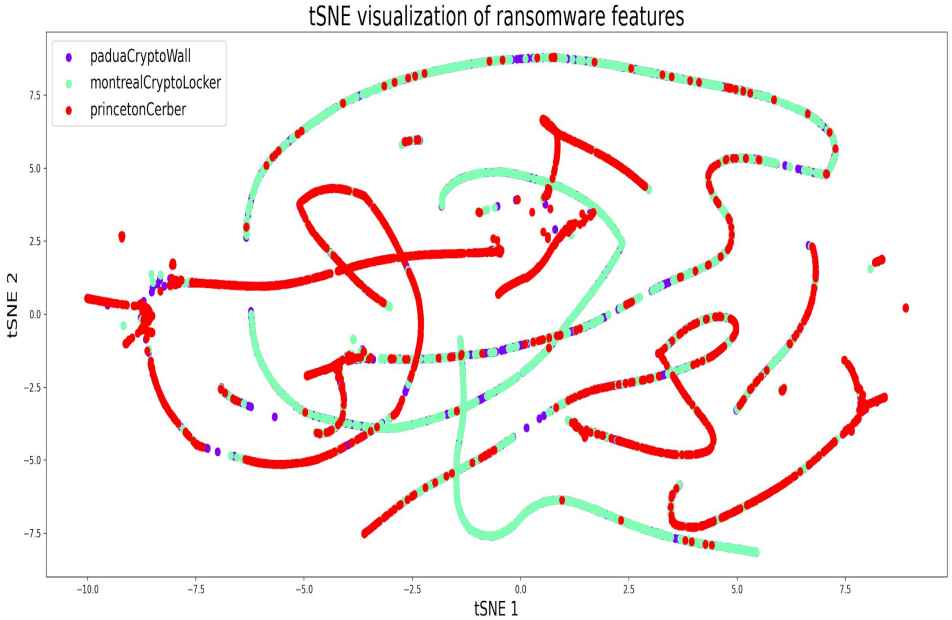
Skewness of the ransomware features







Ransomware clusters using tSNE



Important takeaways

- Clusters of Ransomware firms that separate from non ransomware. Few-shot learning using Topological data analysis can enable us to detect patterns quickly.
- Feature extraction, data selection, date time formatting, clustering and dimensionality reduction.
- Ransomware features different at a global scale but these difference are magnified when looking at the dynamic patterns

Future goals: 1. (Current) Classify new/existing ransomware families from past features and predictions.
2. Implement the few shot transaction pattern learning, which uses meta-learning paradigm.
3. Make it dynamic and scalable using live data.