

Predicting Ransomware patterns in a Bitcoin graph

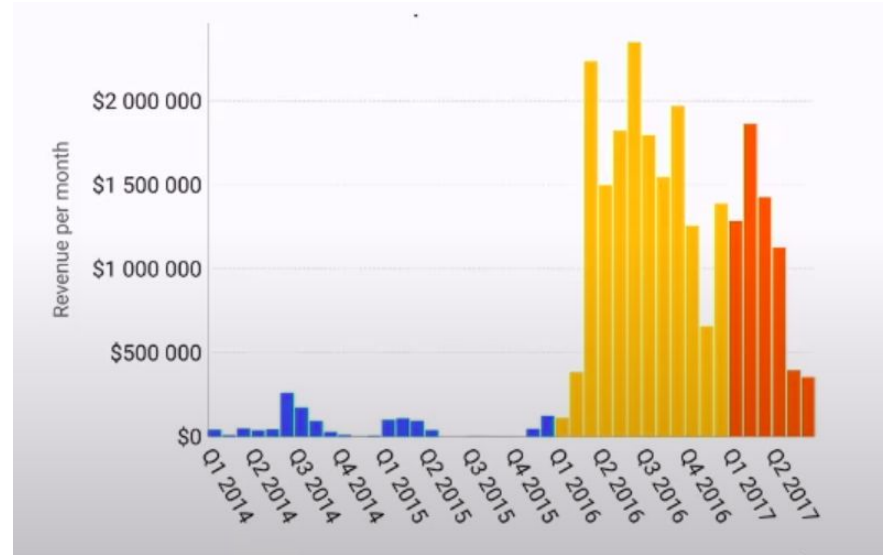
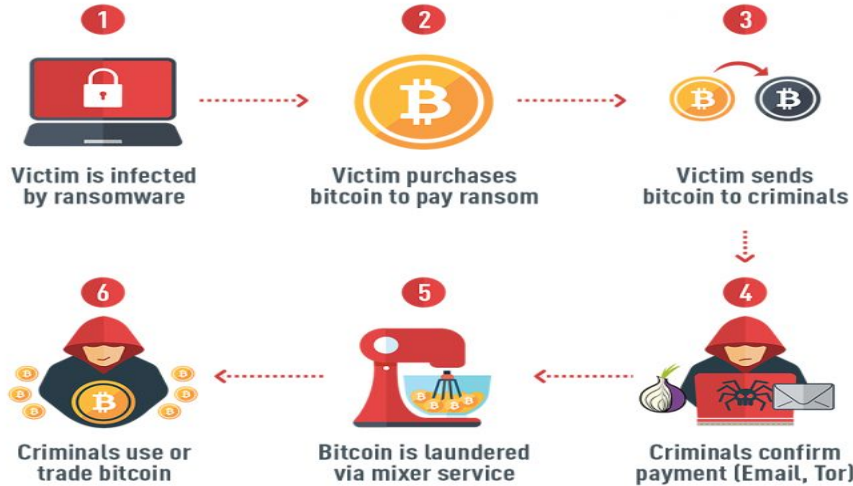
Shannon R. Serrao

[Seasonal variation of Ransomware families](#)

[Github repo](#)

What is Ransomware ?

How ransom payment transactions work



Ransomware hits election infrastructure in Georgia county

By Brian Fung, CNN Business
Updated 4:23 PM ET, Thu October 22, 2020



MORE FROM CNN BUSIN

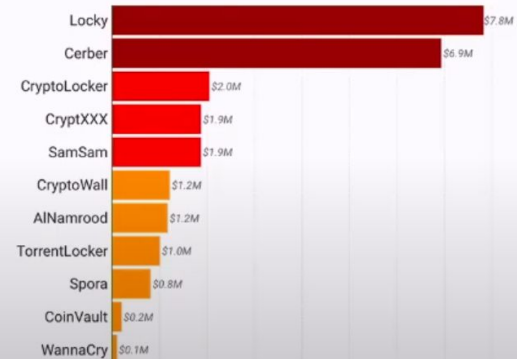
Trump's latest lie is illegitimate to h

See Pete Buttig moments

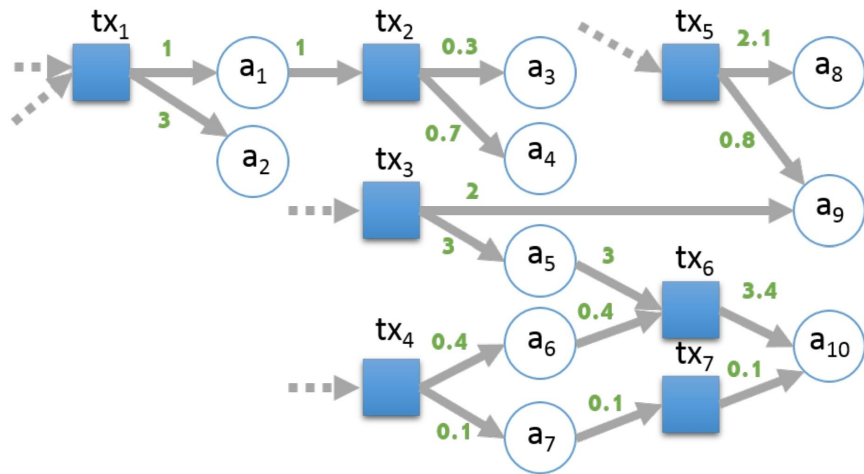
Ad closed by

Report the

Ad choic



Tracking Ransomware on a Blockchain



Features

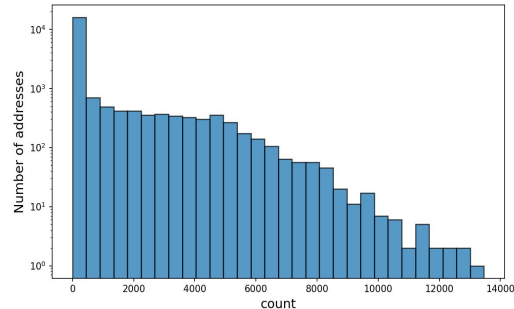
- Count
- Length
- Income
- Count
- Weight
- Neighbors

Dynamic activity of
Ransomware transactions

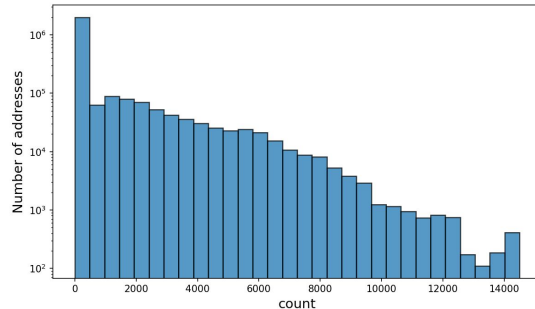
Heroku app: [Seasonal variation of Ransomware families](#)

Skewness of the ransomware features

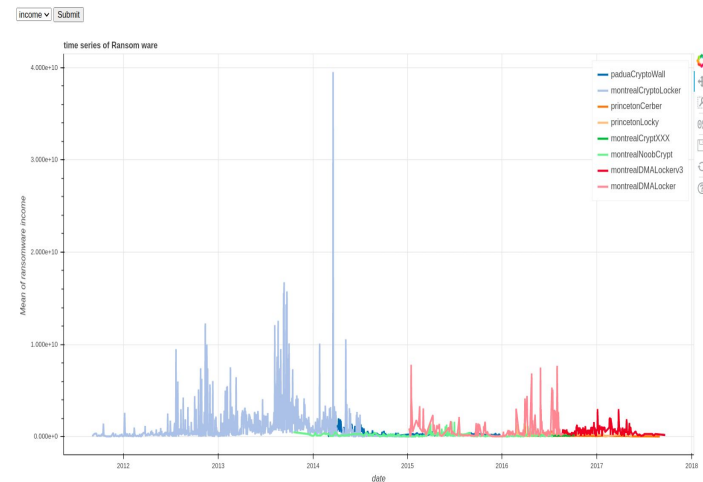
Count distribution in ransomware addresses



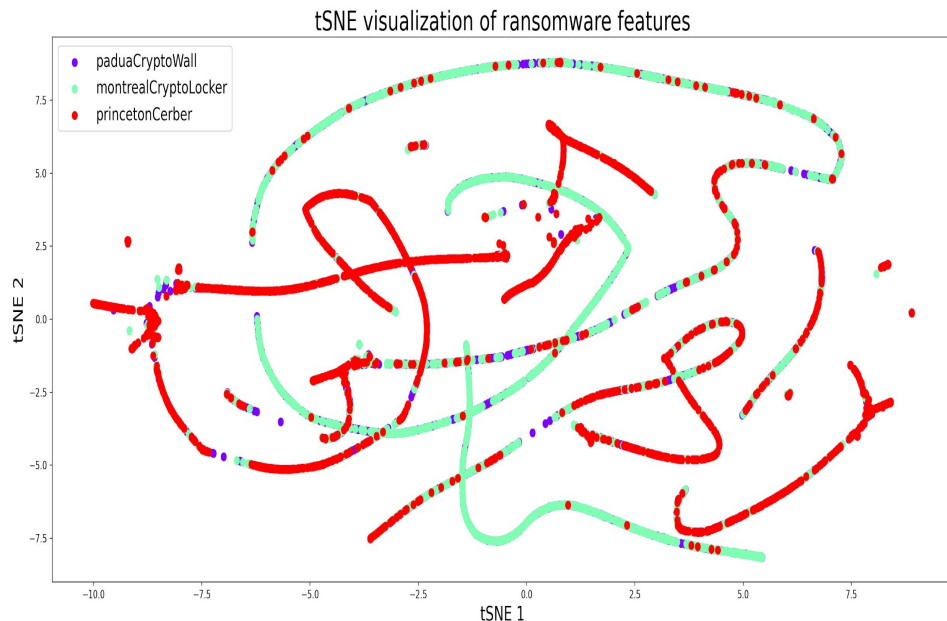
Count distribution in non ransomware addresses



Time plot



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.