SAM ADAMS | METIS 2018

FANTASTIC CYBERATTACKS AND WHERE TO FIND THEM

NETWORK INTRUSIONS ARE COSTLY FOR EVERYONE

- Intrusions are any unauthorized activity on a computer network, either internal policy violations or activity by external agents.

- 145M social security numbers
- $220M in related expenses YTD

TASK: IDENTIFY INTRUSIONS IN SERVER LOGS

Dataset: server logs for 2.5M connections

Process information in logs

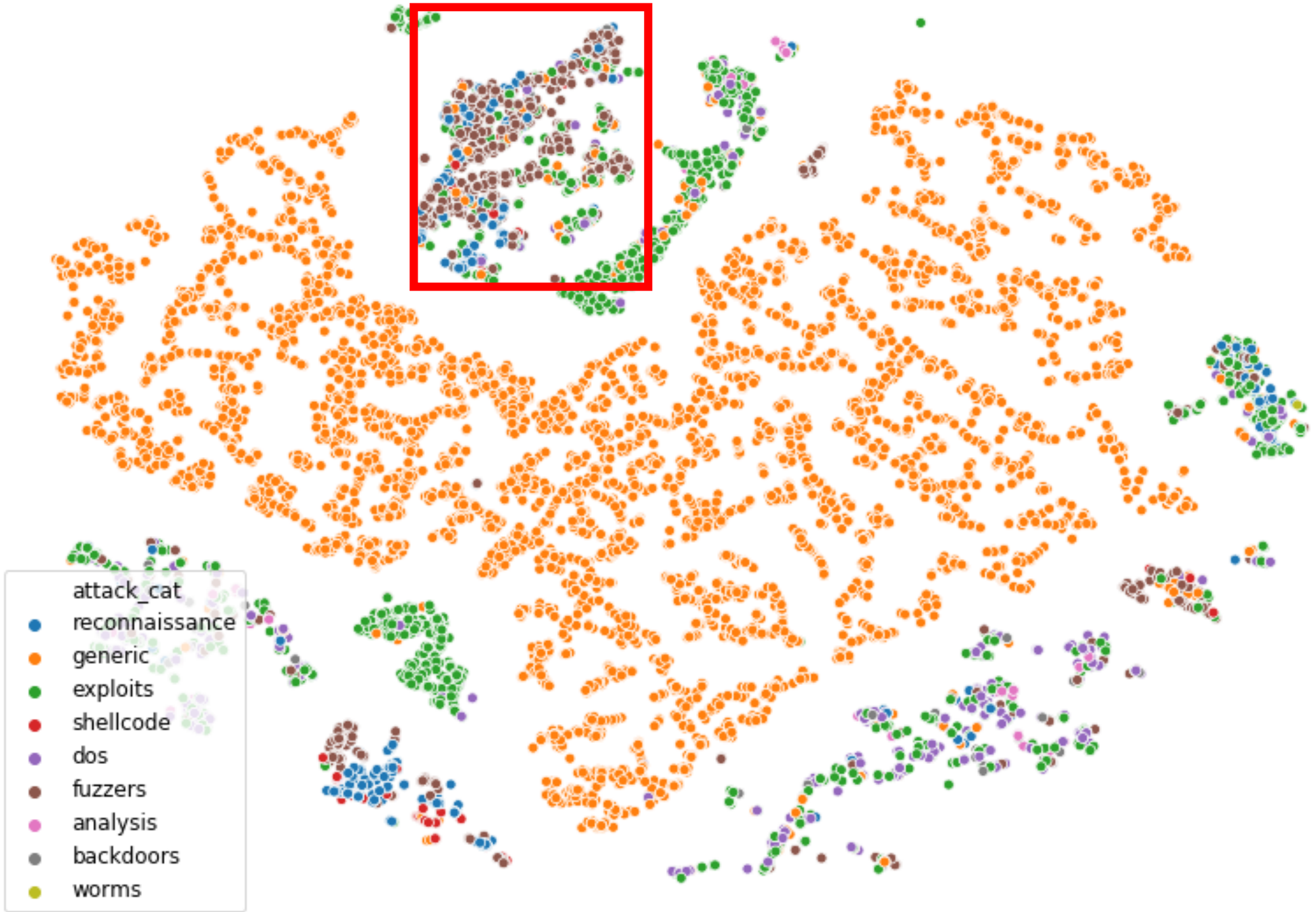
Supervised classification

Unsupervised anomaly detection

FLAG PERSISTENT, HIGH VOLUME CONNECTIONS

- Best performance:
  - Random Forest Classifier, AUC 0.98
- Attack characteristics:
  - Larger than normal data transactions
  - Higher than normal data flow
  - Information is more persistent in the system

DISTINGUISHING BETWEEN DIFFERENT ATTACK TYPES



SPECIALIZE MODELS FOR DIFFERENT ANOMALIES

- Recognize different types of anomalies
- Leverage subject matter expertise to build models that monitor different parts of your network
- Applications in manufacturing, healthcare and financial fraud detection, and more

COME SAY HELLO

Sam Adams

pszadams@gmail.com

psamueladams

adamsxs

APPENDIX

SAM ADAMS | METIS 2018

FANTASTIC CYBERATTACKS AND WHERE TO FIND THEM

REFERENCES

- YTD Expenses: https://www.fool.com/investing/2018/10/25/heres-why-equifax-stock-is-plunging-today.aspx
- Breaches: https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496
- UNSW-NB15 Dataset:
  - Resource: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/
  - Paper: https://ieeexplore.ieee.org/abstract/document/7348942
- Attack Types: see “Kill Chain” methodology: https://en.wikipedia.org/wiki/Kill_chain
-

PHOTO CITATIONS

- UNSW Canberra Logo: https://twitter.com/unswcanberra
-

ANOMALOUS BEHAVIOR IS MORE IDENTIFIABLE WHEN EXAMINING BY CONNECTION TYPES