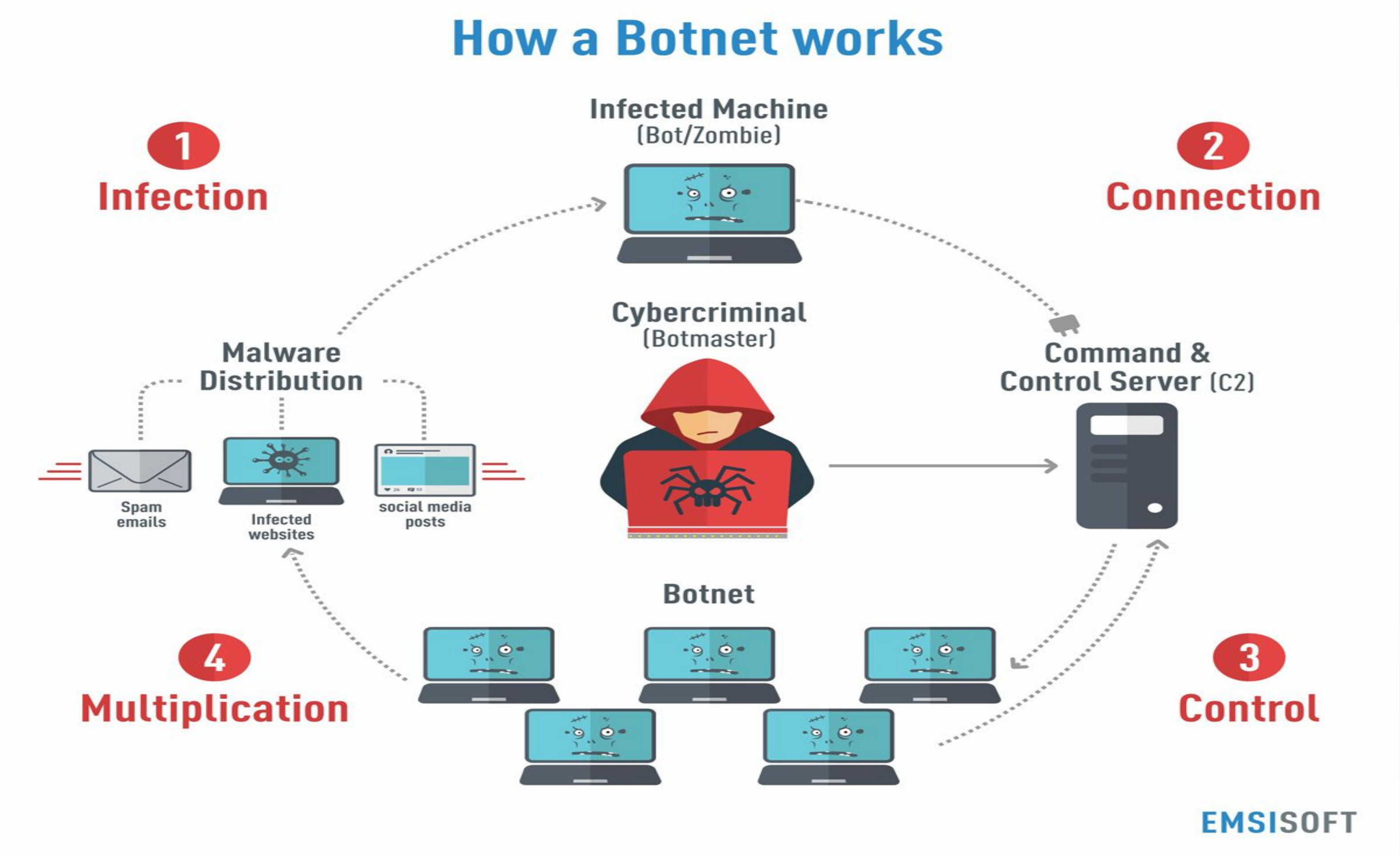
DETECTION OF BoTs (BOTNET OF THINGS)

SUBMITTED BY:

HARJASHANPREET KAUR	B00785792
PRIYA GOSAIN	B00763986

DALHOUSIE UNIVERSITY

BOTS, BOTNETS AND BoT



Source: https://goo.gl/images/hXiXDZ

PROBLEM STATEMENT

Statement-1: To distinguish bots traffic from the legitimate traffic

Data Source: https://web.cs.dal.ca/~haddadi/data-analysis.htm

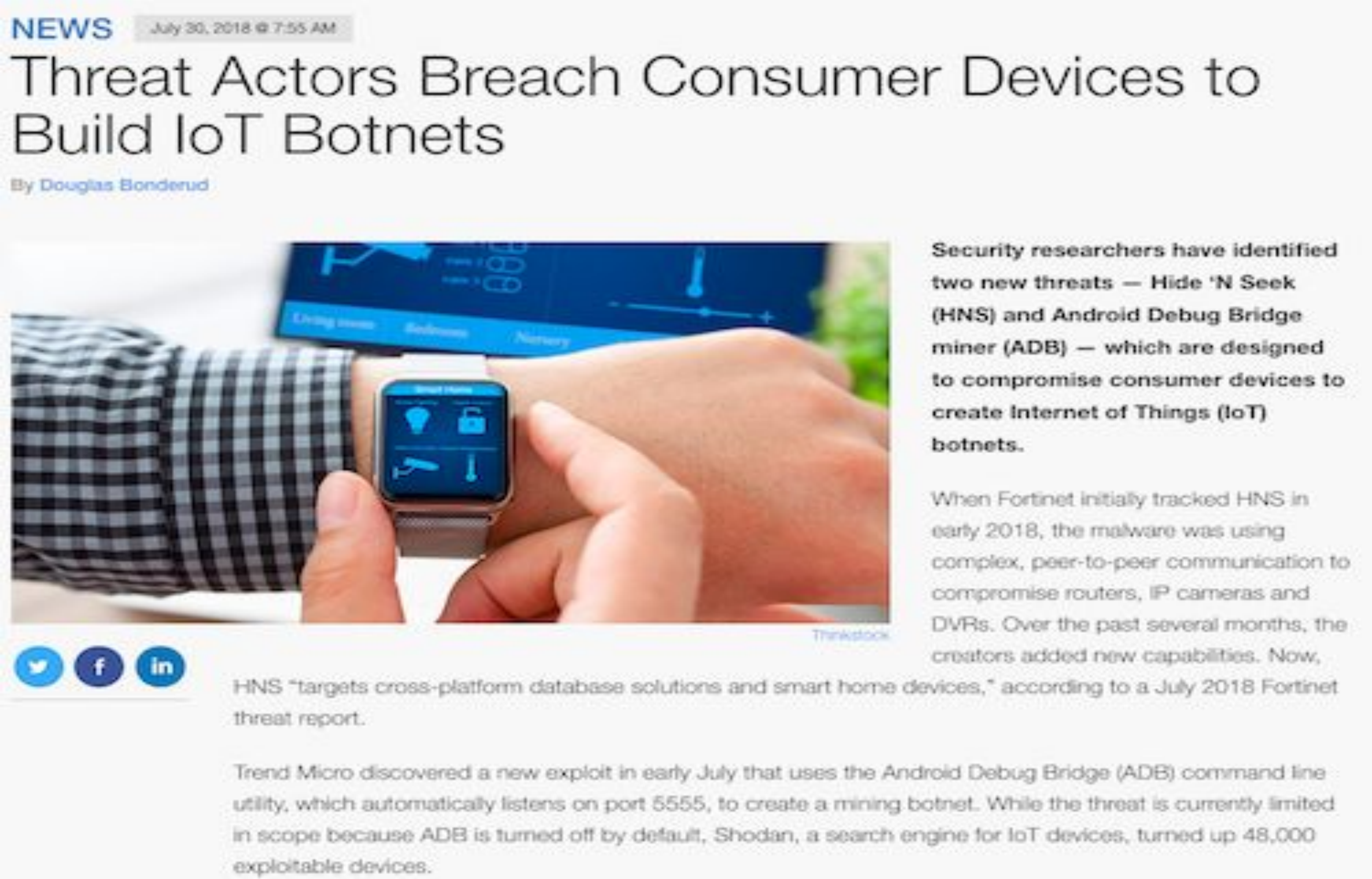
Statement-2: To classify Botnet of Things (BoT) devices

Data Source: https://archive.ics.uci.edu/ml/machine-learning-databases/00442/

VALUE PROPOSITION

Source: https://goo.gl/images/Pir7ZD

VALUE PROPOSITION



NEWS July 30, 2018 @ 7:55 AM

Threat Actors Breach Consumer Devices to Build IoT Botnets

By Douglas Bonderud

Thinkstock

Security researchers have identified two new threats — Hide 'N Seek (HNS) and Android Debug Bridge miner (ADB) — which are designed to compromise consumer devices to create Internet of Things (IoT) botnets.

When Fortinet initially tracked HNS in early 2018, the malware was using complex, peer-to-peer communication to compromise routers, IP cameras and DVRs. Over the past several months, the creators added new capabilities. Now, HNS "targets cross-platform database solutions and smart home devices," according to a July 2018 Fortinet threat report.

Trend Micro discovered a new exploit in early July that uses the Android Debug Bridge (ADB) command line utility, which automatically listens on port 5555, to create a mining botnet. While the threat is currently limited in scope because ADB is turned off by default, Shodan, a search engine for IoT devices, turned up 48,000 exploitable devices.

Source:https://securityintelligence.com/news/threat-actors-breach-consumer-devices-to-build-io t-botnets/

TOOLS & SOFTWARES

Pycharm IDE

Libraries used

- scikit-learn
- pandas
- matplotlib

Graphviz (Graph Visualization Software)

TcpTrace (Feature Extraction Tool)

CLASSIFICATION CRITERIA

Zeus-Alexa Dataset (2 classes)

- Illegitimate
- Legitimate

Bashlite-Mirai Dataset (9 classes)

- Bashlite & Mirai Doorbell
- Bashlite & Mirai Thermostat
- Bashlite & Mirai Baby Monitor
- Bashlite & Mirai Security Camera
- Bashlite Webcam

DATA ATTRIBUTES

Zeus-Alexa Dataset

- Duration
- Total_Packets
- Total_Bytes
- Load
- Rate

Bashlite-Mirai Dataset

- Host_Packets_1
- Host_Packets_2
- HH_Packets_1
- HH_Packets_2
- HH_Jitter_1
- HH_Jitter_2

IMPLEMENTATION

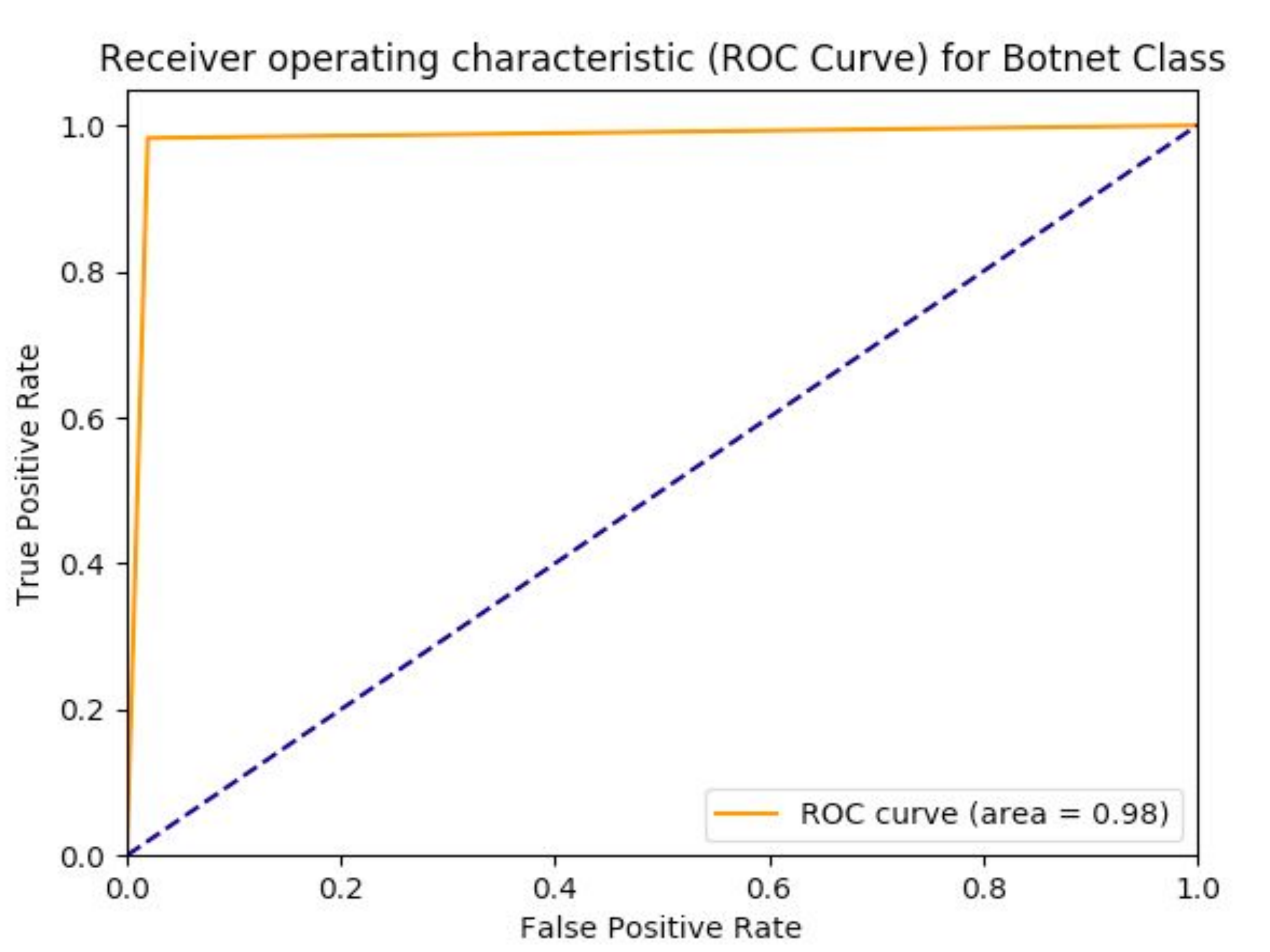
- Predictive Analysis:
  - Decision Tree
  - Random Forest Classifier

- Descriptive Analysis:
  - Graphviz
  - Matplotlib

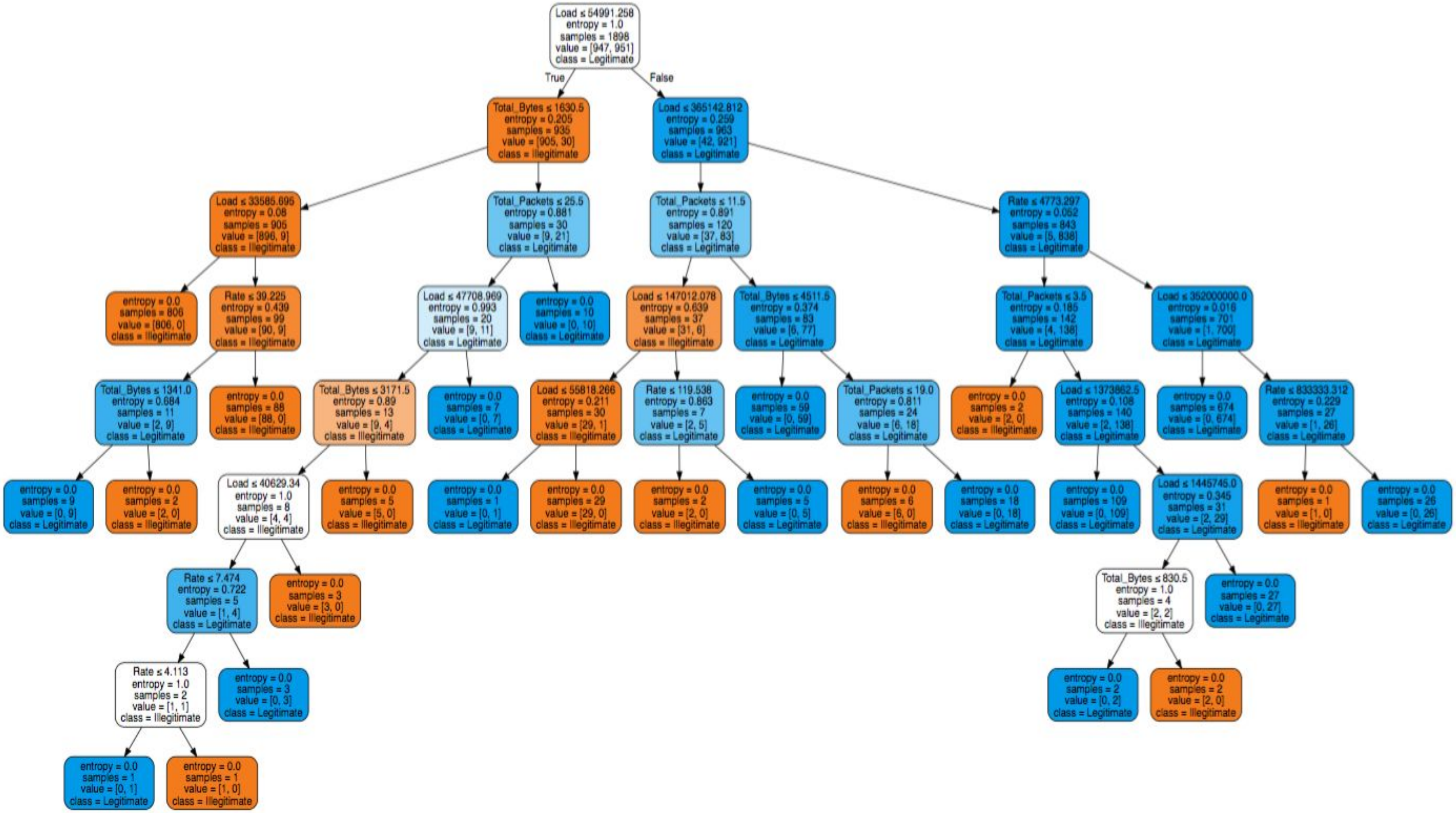
CLASSIFIERS USED

Classifiers	Accuracy (Dataset-1)	Accuracy (Dataset-2)
Decision Trees	98%	72%
LinearSVC	80%	NA
Logistic Regression	40%	NA
Random Forest Classifier	99%	76%

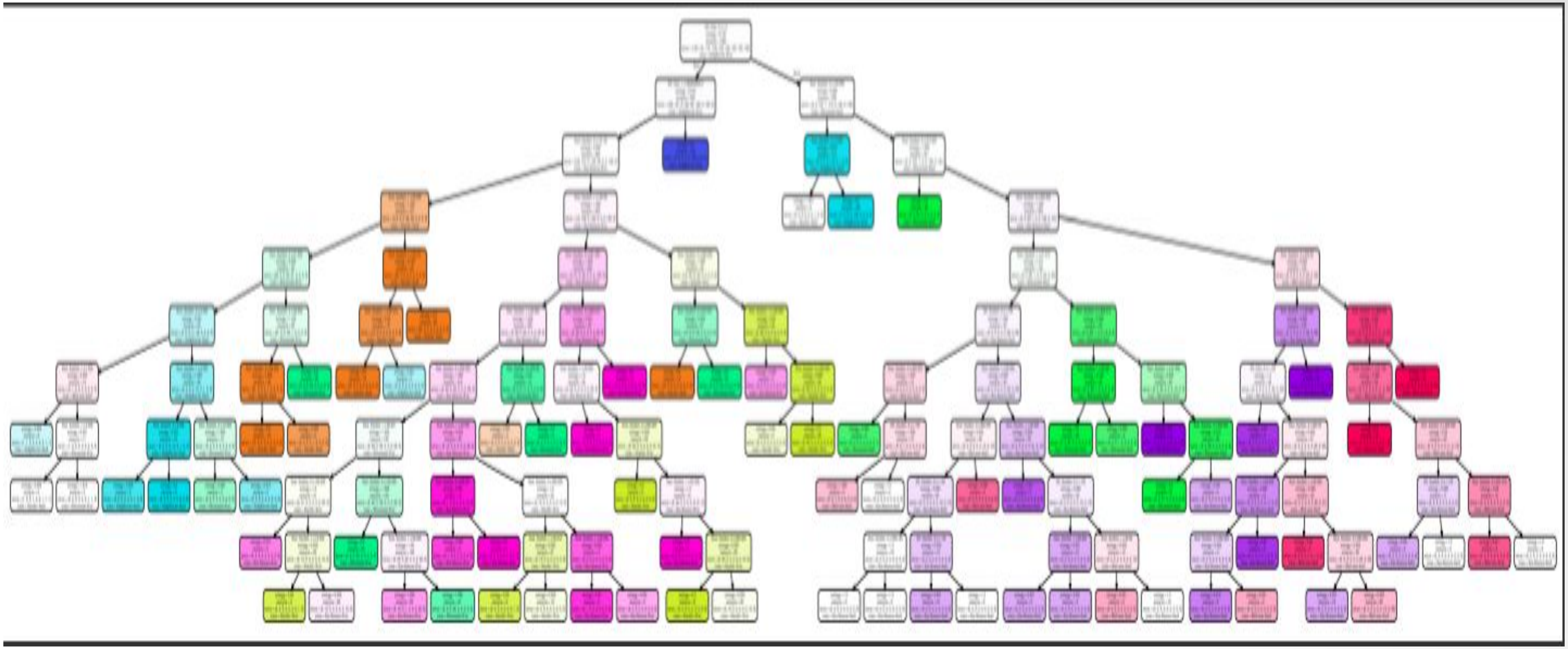
ROC CURVE


Receiver operating characteristic (ROC Curve) for Botnet Class
True Positive Rate
False Positive Rate
0.0
0.2
0.4
0.6
0.8
1.0
ROC curve (area = 0.98)

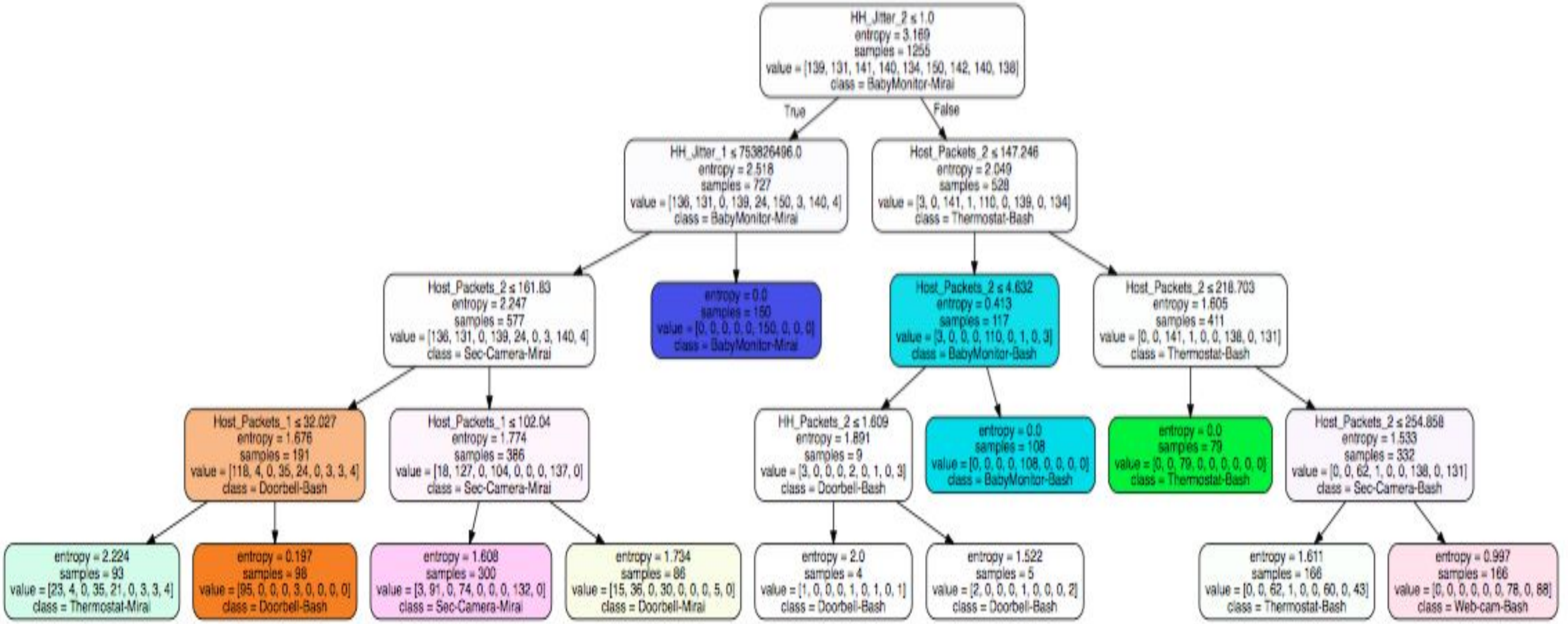
VISUALIZATIONS (Dataset-1)



VISUALIZATIONS (Dataset-2)



VISUALIZATIONS (Max_Depth = 4)



WORK BREAKDOWN

Sprint-1: ETL of Zeus-Alexa dataset

Sprint-2: Train the Classifier

Analysis and Visualization

Sprint-3: ETL of Bashlite-Mirai dataset

Train the Classifier

Sprint-4: Analysis and Visualization

FUTURE WORK

- Study wireshark traffic (real-time analysis) to detect the malicious activity within a network
  - Run the decision rules in real-time to build additional firewall rules
  - Periodic logs of traffic data to report high-priority risks in the network
- Improve upon the accuracy of Random Forest Classifier

ROLES

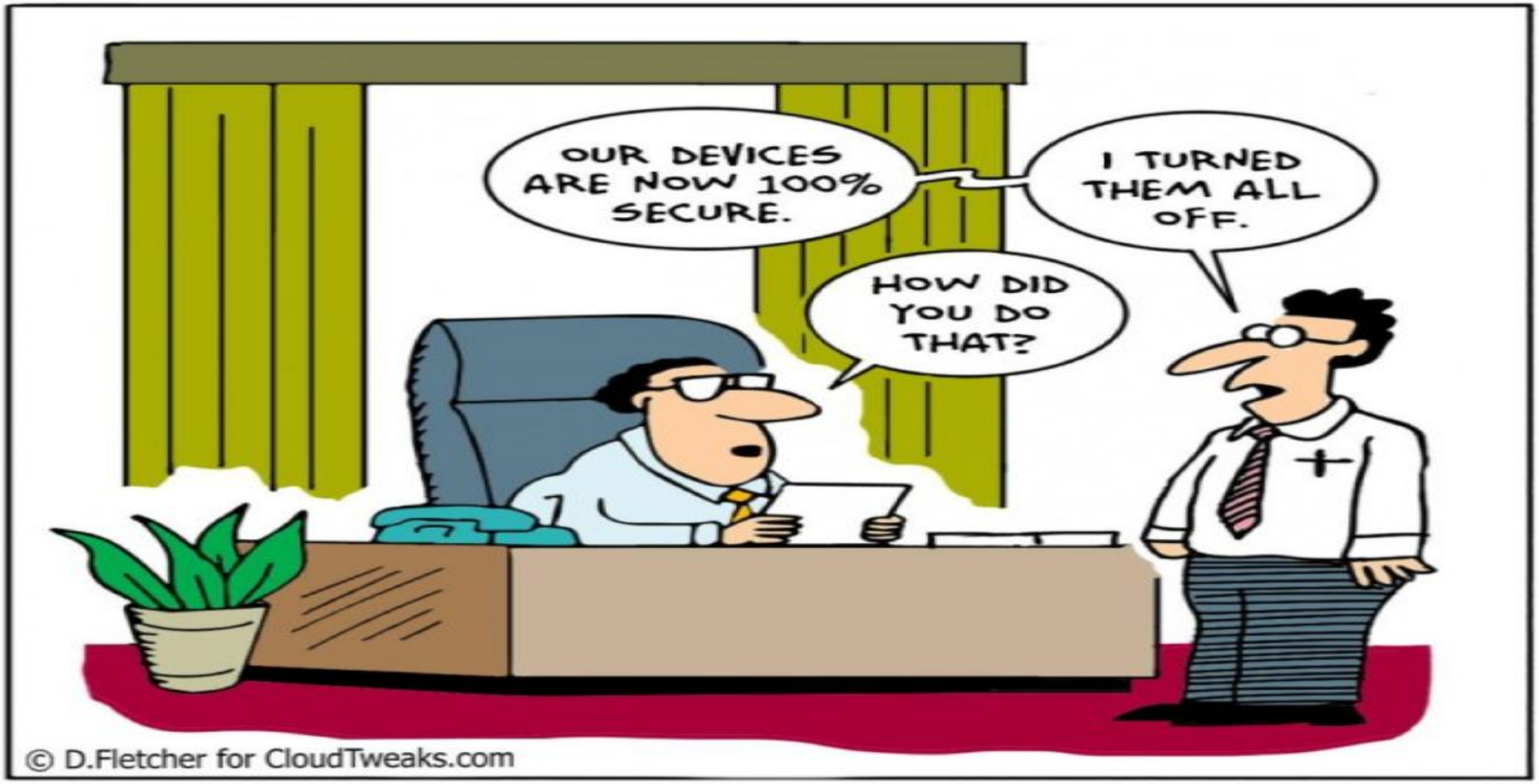
- Data Scientist:
  - Extract and analyze the features
  - Train the model
  - Visualization

- Data Engineer:
  - Test the trained model
  - Cleaning the data

REFERENCES

[1] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A. and Elovici, Y. (2018). *N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders*. [online] Arxiv.org. Available at: https://arxiv.org/abs/1805.03409v1 [Accessed 2 Aug. 2018].

[2] Sans.org. (2018). [online] Available at: https://www.sans.org/reading-room/whitepapers/detection/decision-tree-analysis-intrusion-detection-how-to-guide-33678 [Accessed 2 Aug. 2018].


OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

THANK YOU!

Source: https://goo.gl/images/waaLGW