**Name**

Samah Taher Abdo Ebrahim

**Student number:** 300273128

**Paper title:**

Real-Time Detection of DNS Exfiltration and Tunneling from Enterprise Networks

**Authors:**

Jawad Ahmed, Hassan Habibi Gharakheili, Qasim Raza, Craig Russell, and Vijay Sivaraman

## ◦ Summary

### Problem :

DNS communication is relatively poorly policed by organization compared to other services and that make it exploited by cyber-criminals to maintain covert communication channels and has the ability to make data exfiltration to access very private and sensitive information which accordingly caused huge resulting damages can be, amounting to several million dollars in a single attack, so the challenge here is to develops and evaluates a real-time mechanism for detecting exfiltration and tunneling of data over DNS

### Solution :

The proposed solution includes first feature extraction from the domain name of the collected data. these features are stateless which is independent of the time series such as FQDN in which the total number of characters is calculated and also other features like uppercase, lowercase, label count,...and so on. Then providing these features to a machine learning model to make analysis and classify whether it is malicious or not, they used the iForest algorithm that isolates observations by randomly selecting an attribute and then randomly selecting a split value in the range of values

### Experiments

They go through some experiments in two different organizations (research institutes and university campuses)to get progress, first using three the tuning parameters for iForest during the training phase namely a number of trees (n estimators), height limit of trees (max samples), and contamination rate. They use the value of each parameter
while fixing the other two parameters and validating the accuracy of their model for both benign and malicious instances, and after some tries, they found the optimal value of tuning parameters equal to 2, 18, and 2% respectively for the number of trees, the height limit of trees, and the contamination rate.

### Results

To evaluate their performance they used three different metrics: accuracy, Real-Time Performance, and Known DNS Exfiltration. And the results show that

the rate of false alarms is mostly less than 5% in both organizations, though we see a higher false rate (i.e., more
than 10%) and can be seen that 98% of benign instances are
correctly detected as normal during both cross-validations (i.e.,
Days 1-4) and testing (i.e., Days 5-7) phases. Also in terms of DNS exfiltration, their machines for the Research Institute and the University Campus respectively were able to correctly detect 95.07% and 98.49% of exfiltration queries (generated by our DET tool) as anomalous instances.

### conclusion

stealing valuable and sensitive data over DNS channels leads to results devastating results they have developed and validated a mechanism for real-time detection of DNS exfiltration and tunneling from enterprise
Networks. They evaluated the efficacy of their scheme on live 10 Gbps
traffic streams from the borders of the two organizations' networks by injecting more than a million malicious DNS queries via an exfiltration tool

## ◦ Critical Review.

### Research Goal

The authors tried here to answer questions like what are important features machine learning models could analyze to detect attacks in DNS ? what metrics should we depend on to get satisfying results?

### Clarity

The paper is easy to follow and understand everything is street forward for that who have a background in machine learning

### Related Work

The related work is adequate but it is not enough for those who do not have previous information about security so far it is clear and the authors provide a special section for acknowledgments for their collaboration with the Australian Defence Science and Technology Group.

## Methods

They used iforest algorithm as a method for classification and they illustrate its special way for analyzing features but probably they missed to talk more about the difference between that algorithm and the others and why they use it particular

## Results and Claims

The paper provides applied results which they get from two organizations illustrated in tables and figures in a nice way, According to claims their initial objective is to provide good results for anomaly detection and they already meet that with accuracy 97.99% for Benign domains and 70.57% for others

## Support of Results and Claims

They already support their claims by visualizing the results they achieved and describing their tries like tuning parameters and also providing different evaluation metrics to evaluate their model

## Missing Claims and Results

To improve the results and meet their claims, stateful features are also needed beside stateless ones to simulate a real-life scenario a security-wise, also trying different models with different datasets to generalize the results in a large scope

## Discussion

As overall the discussion is very clear and well written which make it easy to follow and contribute with