University of Ottawa
Faculty of Engineering
School of Electrical Engineering and Computer Science

CSI5388/ELG5271/ELG7186: Assignment 1

Student name: Hosam Mahmoud Ibrahim Mahmoud
Student number: 300327269

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

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

A. Summary

- The **problem** that the authors of that research paper tried to solve is to protect enterprises from Domain Name System (DNS) exploitation and data exfiltration. knowing that DNS is a protocol that is not very well monitored from a security perspective compared to services like FTP and HTTP.

- The authors **solved** this problem by developing, tuning, and evaluating a real-time anomaly detection solution for detecting data exfiltration, and data tunneling over DNS.

- The **experiments** that the authors of this research paper done Are:
  1- The authors *Developed, tuned, and evaluated* a real-time anomaly detection solution over DNS queries using a benign dataset and other datasets that the authors have collected from a mid-sized Government Research Institute and a large University, the authors collected 7 days of data, and the authors trained their model on the 4 days' worth (1-4 days) of data and tested their model on the remaining data (5-7) days.
  2- The authors *implemented* their solution on live traffic from networks of the research institute and the university, to *test* if their solution would detect the anomalies in DNS queries with acceptable accuracy or not.

- The **result** that the authors have got after **developing, tuning, and testing** their model is:
  Stable and effective real-time solution for the proposed problem and this solution gave them good results in terms of speed and accuracy, and this will be discussed in detail in the Results and Claims section

- **The main conclusion:** is that the authors have developed a model that can detect real-time DNS exfiltration and tunneling from enterprise networks, with relatively high speed and accuracy.

B. Critical Commentary of Paper

- **Research goal**
  - The research goal is to develop a real-time solution that can protect enterprises from attacks that exploit DNS channels to exfiltrate data and do bad things, with good accuracy compared to the methods that require temporal states to query names or the activity of the DNS host.
  - Depending on the attributes that the authors have identified for query names which are:
    1-Total count of characters in FQDN, 2-count of characters in sub-domain, 3-count of uppercase characters, 4-count of numerical characters, 5-Entropy which is: a measure to determine if the string is readable or not, 6-number of labels, 7-Maximum label length, 8-Average label length.
    Are the authors would be able to provide a solution that will detect these attacks before it's happened in real-time with good accuracy?
    I think these attributes defined the critical differences between the normal query names and the anomalous ones, and I think that their model gave good results in terms of speed and accuracy.
- **Clarity**
  - The paper is relatively clear and to the point, but for people who don't have a technical background in security, I think it won't be easy to understand what's going on.
  - For the ones who know about machine learning they will understand the machine learning concepts in that paper: like the parameters of the "Isolation Forest (iForest)" and how the authors tuned these parameters, but for security concepts, I think it needs more clarification.
- **Related Works**
  - I think that the authors mentioned related topics to what they have proposed.
  - But I think that the related work section is missing some details like, the authors did not mention the accuracy of any paper, and more than a quarter of this section is about their project, making the related works section short.
  - The authors mentioned good details about the contributions of the others' works like which algorithms they have used, but the authors did not mention the others' results.
- **Methods**
  - the authors have collected the data which is domain names, after that, the authors defined some attributes to be able to work with these Fully Qualified Domain Names, after that, the authors developed a real-time anomaly detection model which is "Isolation Forest (iForest)" using python with scikit-learn, after that, the authors do a hyperparameter tuning to increase the detection of anomalous queries as possible as they can and trying to reduce the rate of false results as possible as they can, after that, the authors have evaluated the effectiveness of their real-time solution by:

1- test the model on benign instances to get the baseline accuracy of the model that was trained before and apply cross-validation technique on that model, 2-determine and test the detection rate for the anomalous (malicious) domains, and 3-testing the performance in real-time by trying this model on live traffic on the networks of the two organizations.

  - I think the above methodology answered the question that the authors tried to answer before by having good results in terms of speed and accuracy. (the question is mentioned in the research goal in the 3rd point).
  - The details that the authors have mentioned about their methodology are clear and to the point.

- **Results and Claims**
  - For the applied results, 1- Their model took around 800 microseconds to determine if the query name is malicious or not, which means that their model can process about *1250 query names (DNS query) per second.*

    2- For the accuracy of the test data that belong to the *Research Institute and the university respectively* (5-7 days' worth of data), their model detected *98.30%, 97.99%* of *Benign domains* as *normal,* and *1.70%, 2.01%* as an *anomaly*, and for *other domains'* test data, *77.55%, 70.59%* were detected as *normal,* and *22.45%, 29.41%* as an *anomaly.*
  - The authors claimed by saying "We believe that classification (signature-based) approach is not sufficient for addressing the new and growing security issues" this claim.

    The second claim is they have said that something like a one-class SVM or Replicator Neural Network would not be good for this problem.
  - At the begging the authors said that they would build a real-time solution to solve the proposed problem and they have achieved it.
- **Support of Results and Claims**
  - For the first claim the authors did not prove or talk about why the classification (signature-based) approach is not sufficient.

    For the second claim, I think they have proved their point of view theoretically.
  - The authors clarified that the Benign domains are considered as the baseline dataset and it does not contain any malicious domains.

    But on the other hand, they did not mention the proportion of normal and malicious domains in the other dataset, for example by knowing that 77.55% were detected as normal and 22.45% were detected as an anomaly, I can't judge if these accuracies are good or bad because I don't know the proportions for this dataset.
  - I think the authors did not do any experiments regarding the claims that I've mentioned above.
  - the authors empirically evaluate their work, as mentioned in detail in the methods section.
  - As they mentioned before, such a solution could save enterprises millions of dollars, and they have tested their solution on the networks of two big organizations and it gave good results.
- **Missing Claims and Results**
  - I think the authors should try different anomaly detection algorithms like Local Outlier Factor or Robust Covariance.
  - After adding more algorithms, they should make comparisons between different algorithms and add more visualizations for the comparisons, I think that would make the paper better.
- **Discussion**
  - Actually, this paper does not contain a section called "discussion". the authors should provide this section to analyze, explains, and summarizes the whole procedure in a simple manner.
  - Because of missing the "discussion" section readers may not be able to see all the connections between each section of this paper.
  - The authors mentioned the speed of their real-time solution as a strength for them, but I think that they did not mention any weakness in their research, but I believe that they should be taking at least another algorithm into consideration to be able to make a comparison between two or more algorithms.
- **Future work**
  - I think taking other attributes like the temporal states of that host that generate malicious DNS into consideration and taking different anomaly detection algorithms into consideration, would be reasonable to do in the future.