**Detecting Malicious DNS over HTTPS Traffic in Domain Name System using Machine Learning Classifiers**

* Project Title:

Detecting Malicious DNS over HTTPS traffic in DNS using Machine Learning Classifiers.

* Motivation of the project:

The main aim of the project is to increase user privacy and security by preventing attacks and manipulation from attackers by detecting and differentiate malicious or normal traffic using Machine learning models such as Navie bayes, support vector machine, random forest, and neural network regression.

If we are successful in differentiating the malicious and non-malicious DoH, we can prevent the attacks such as man in the middle attacks and many more.

* Description of problem we plan to address

In this project, we are planning to detect and differentiate the malicious DOH and normal DOH packet. The packets will be encrypted using the HTTPS protocol between the DOH client and DOH based DNS server.

* Why is this problem challenging?

As the DoH offers a new opportunity for users' privacy, it makes a way for malware developers. If DNS requests are encapsulated and encrypted using DoH, these requests will be extremely hard to identify the malicious and normal packets.

Later we will try to classify the domain generating algorithms DGA related DOH traffic from other HTTPS traffic. Botnet uses the fast domain fluxing or domain generating algorithms and abuse DoH.

* A paragraph description of papers that addressed the same problems.

The papers used machine learning classifiers to differentiate DoH and Non-DoH traffic so that they could prevent attacks and increase the user's privacy and security. And they were able to achieve high precision, F1 and recall results of 99.3%.

1. Classifying DNS Tunneling Tools for Malicious DoH Traffic Rafa Alenezi; Simone A. Ludwig

Date of Conference: 05-07 December 2021

The paper focused on investigating the machine learning models for solving the DNS tunneling and DoH security problems. They used the classifiers to detect the DNS tunneling of DNS attacks in DoH traffic.

2. An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) Attacks

Zebin, Tahmina, Rezvy, Shahadate and Luo, Yuan

Published on: 09 Jun 2022

In this paper they proposed the AI solution using a novel machine learning framework to classify the DNS over HTTPS attacks. They use the publicly available CIRA-CIC-DoHBrw-2020 dataset for developing an accurate solution.

3. Feature Engineering and Machine Learning Model Comparison for Malicious Activity Detection in the DNS-Over-HTTPS Protocol Matthew Behnke; Nathan Briner; Drake Cullen; Katelynn Schwerdtfeger; Jackson Warren; Ram Basnet; Tenzin Doleck

Date of Publication: 16 September 2021

The paper uses the publicly available dataset and compares 10 different machine learning classifiers for 10-fold cross validation. Those were used to classify the malicious DNS over HTTPS traffic.

4. Detection of DoH Tunneling using Semi-supervised Learning method Anh Tuan Nguyen; Minho Park Published in: Jan 2022 International Conference on Information Networking (ICOIN)

Proposed the semi supervised machine learning classifier to detect malicious DoH tunneling. They first collected the DoH traffic and labeled them. And evaluated the classification efficiency using the semi-supervised algorithms. And was able to distinguish between the DoH tunneling from HTTPS traffic.

5. Detecting Malicious DNS over HTTPS Traffic in Domain Name System using Machine Learning Classifiers

Yaser M. Banadaki

Published on: August 20, 2020

The paper uses machine learning classifiers such as Naïve Bayes, Logistic Regression, Random Forest, K-Nearest Neighbor and Gradient Boosting to detect the malicious activities in the DoH. And concluded that the ML-based algorithms are best options for prevention of the DNS attacks on DoH traffic.

* Short comings:

The previous work only used six classification algorithms such as Decision tree, Extra tree, Gradient Boosting, XGBoost, Random Forest and SVM (Support Vector Machine). We will try to deploy more algorithms to get different and more accurate results.

The precision recall and F1 score of Naïve Bayes were too low compared to other classifiers.

* Dataset:

we are planning to use publicly available CIRA-CIC-DoHBrw-2020 dataset. Canadian Institute for Cybersecurity (CIC) project funded by Canadian Internet Registration Authority (CIRA). The dataset can be found here <https://www.unb.ca/cic/datasets/dohbrw-2020.html>

* Procedure/Tools details:

We are planning to detect and differentiate the malicious and benign in DoH using Machine learning classifications. We will also try to use deep learning at the end. To train our machine learning models we will be using libraries such as Pandas, pyplot, sklearn, pydotplus.

We will be using the AI based algorithms to distinguish the DGA related DOH traffic from other HTTPS traffic.

Random forest classifier, extra tree classifier, naïve biased, K-Neighbour classifier are the algorithms, we will try to fit our dataset on these models and see how they are performing, based on the results we will try to use different algorithms.

XGboost, GradientBoosting, and Light Gradient Boosting algorithms are used to boost the accuracy of the previous models if they are not working well.

* Metrics:

The ML model Navie Bayes is not performing well when it comes detecting malicious and benign DoH, we will try to train this model with various methods like forward feature selection and backward feature selection. (Not 100 sure, but we will try our best).

Planning to use wrapper methods which will help our models score.

* Data cleaning:

We will be following the regular data cleaning process, removing the duplicate observations, filtering the unwanted outliers, and fixing missing data..etc.