---------- CM3203 Individual Project (40 Credits) ----------

Initial Plan - Is COVID-18 Being Used to Spread Malware?

Author: Izabele Bauzyte, Supervisor: Amir Javed

Project Description

39% of adults in the U.K. use social media as a source of news (Watson). Coincidentally, 39% of U.K. individuals also report being 'very sceptical' of information they read via social media (Daily Question). Despite general scepticism about news and information received from social media, it's use is still widespread. But as popularity increases, so does malicious intent.

One particular sphere, information relating to COVID-19, has recently seen a fair amount of malicious redirection and misinformation. Links to "Corona Antivirus" infect users with a BlackNET RAT malware which can execute harmful scripts and even launch DDoS attacks. Links to pages masquerading as official government websites collect users' personal information and bank details (Developing Story). The list goes on. Fortunately, this public information can be analyzed to determine malicious intent and find groups of users spreading certain links. With vast amounts of information being published to twitter everyday, it is important to monitor this information and mitigate harm. Twitter data collection and user analysis will be the basis of this project.

This project will involve the collection of public twitter posts relating to COVID-19. The data will be analyzed to find links redirecting to malicious web servers and checking if tweets marked as 'malicious' contain misinformation in order to clickbait users. Finally, supervised machine learning will be used to attempt to identify whether a tweet is malicious or not.

Aim

The aim of this project is to gather evidence of malicious activity on an online social media platform (Twitter), and to identify key features that could be used to distinguish between malicious and benign posts via supervised machine learning. Namely, we will first determine if a tweet is malicious, and then whether it contains misinformation or not.

Objectives

1. **Data Collection:** First, data collection will be done using twitter as the social media platform. Twitter was chosen for several desirable properties: it has a hashtag system in place that is widely used by users, and will make it easier to find event specific posts, also, the twitter character limit is set at 280 characters, meaning a predictable data size for tweets. A script will be written to establish a connection to Twitter streaming API to collect data using event specific hashtags. This data will need to be stored in a data store and processed for the next step.
2. **URL Classification:** Any URLs contained in the data will be segregated into benign and malicious URLs using either the Virus Total API or Cuckoo Honeypot
3. **Analysis of Tweets:** The malicious tweets will be analyzed for likeness using content and account based features such as emotion, sentiment, number of followers, etc.
4. **Tweet Classification:** Supervised machine learning will be used to classify the tweets into either malicious or benign categories.
5. **Disinformation Classification:** A desirable objective will be to classify tweets that contain malicious urls into further categories: whether or not they contain misinformation intended to mislead or clickbait the users.

Ethical

There aren't many ethical concerns related to the project, as all tweets collected will be public information that is available on the internet. All data collected is publicly available, and doesn't contain sensitive information related to each user.

Timeline

Data Collection and Processing	
Week 1	Initial Plan, background research on pulling data from twitter and determining malicious links [create necessary dev. account]
Week 2	Start pulling data, background research on similar projects and also deciding between using Virus total or Cuckoo Honeypot for URL analysis
Week 3 - 5	Set up data store, import twitter data, pre-processing of data set by connecting with Virus total API/Cuckoo Honeypot and segregating malicious and benign URLs Create a python/Java based program that will preprocess data and create a machine learning input file containing a set of features (features will be identified in week 2)
Building a Supervised Machine Learning Model	
Week 6 - 8	Building supervised machine learning model in python/java to categorize tweets into either “malicious” or “benign” based on user features
Easter weeks 1-3	[CATCH UP] on previous weeks work if falling behind, otherwise maybe try to push ahead
Week 9	[IF EXTRA TIME] Try to reuse code to now categorize malicious tweets into those that contain misinformation or not.
Week 10	[IF EXTRA TIME] Try to reuse code to now categorize malicious tweets into those that contain misinformation or not.
Final Report Work	
Week 11	Finalize documentation based on project notes, analysis for final report
Week 12	Finalizing final report

Bibliography

"Daily Question: 18/06/2020." YouGov, yougov.co.uk/topics/technology/survey-results/daily/2020/06/18/a9715/2.

"Developing Story: COVID-19 Used in Malicious Campaigns." Security News, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

Watson, Amy. "Usage of Social Media as a News Source Worldwide 2020." Statista, 23 June 2020, www.statista.com/statistics/718019/social-media-news-source/.