Capstone Project II Proposal
by Helga Wilde

Detecting Malicious Web Links

Objective

The objective of this study is to classify a web page (url) as benign, spam, phishing or malware, and to identify the minimal set of features that can be used to accurately make these classifications.

Background

Threat actors continue to leverage malicious urls for reconnaissance, initial device access and exploitation purposes.

A malicious web page may compromise the victim's web browser using an exploit, or the user may be motivated to download software, files, or executables. Threat actors may also include links that interact directly with an email reader, with the intention of exploiting the victim system directly. The link may be invisible to the victim (ie web bug or beacon) and will communicate back to the actor's web server once an email is opened. Links may also direct users to malicious applications designed to acquire access tokens which may provide an avenue to protected applications and data.[1]

To protect against malicious urls, inspection approaches include 1.Comparing a url to a url or domain blacklist and 2. Heuristic-based analysis of the communication between client device and the url's web server, and/or analysis of specific web page features.

Clients

The machine learning model may benefit:

- Security vendors with email filtering, web filtering, intrusion prevention, packet capture products.
- Cyber threat intelligence vendors. They may expand on model to include attribution.
- Enterprise security operation teams. They may leverage a predictive model within an in-house or Security Orchestration Automation and Response (SOAR) platform, to evaluate and detect/respond to malicious links in email and/or web traffic.

The Data

1. Benign urls:
   A list of benign urls will be collected by crawling Alexa top websites. These web url links will be submitted to VirusTotal.com to verify that 50+ AV vendors give the page a clean rating.
2. Phishing urls:
   The PhishTank.org website maintains, on average, a list of 17,000+ verified phishing urls currently active and online. This data set includes the following features: id, url, submission datetime, verified status, verification time, online status, target.

[1] "Phishing," MITRE, 02 Mar 2020, Web, 19 Aug 2020.

3. Spam urls:
   Urls will be retrieved from shadowserver.org. Features available include url, hostname, IP, ASN, IP country, and various email attributes.
4. Malware urls:
   The URLhaus project operated by abuse.ch provides csv files of online malicious URLs. Features include id, date added, url, url status, threat, tags, reporter.

Approach and Deliverable

Additional features will be created, based on url links:

URL lexical features
Link popularity
Domain name properties
IP address properties
WHOIS properties
Blacklist membership
Geographic properties
Webpage content

A supervised learning multi-label classification method will be used. The final deliverable will be available in a Github repository and will include:

1. Code, including data acquisition, preparation, EDA, statistical analysis, model
2. A 15-20 page written report and slide deck covering the problem, approach and findings