CS 419/DADA

Week 7 - Lab 2

Michael Depuy

Jonathan McNeil

Marie Caswell

Our team approached the lab by first coming up with a set of rules that would indicate a possibly malicious website. Then we assigned ‘points’ to each URL based on our rules.

Some URL characteristics we counted as suspicious were:

* A domain age less than 188 days.
* TLD not from a common domain like ‘com,’ ‘net,’ or ‘org.’
* An Alexa rank greater than 1000000, or no Alexa rank.
* A domain having greater than three tokens.
* A difference between the registered domain location and the mail exchange location.
* ‘Bad’ file extensions (like .pdf files).

A website reaching a certain point threshold (yet to be determined) will be considered malicious.

We also considered avoiding false positives by awarding ‘safety points’ — meaning that if a URL has characteristics indicating legitimacy (like being located in the same region it was registered) the URL could gain points back.