The Generation of Phishing Domain Names with a Recurrent Neural Network

Kaspar Hageman

August 28, 2018

1 Introduction

This report describes the development of a recurrent neural network for the generation of phishing domain names.

1.1 Covered course material

The primary course material that inspired the project was the introduction to PyTorch by Adam Paszke. Experience with tools in other machine learning course was primarily with `MATLAB` and `scikit-learn`, motivating me to use PyTorch for this project.

The demonstration of a recurrent neural network for the generation of sentences based

1.2 Phishing domain names

In phishing attacks, an attacker - or phisher - attempts to obtain sensitive information from its victim through digital means. A common phishing attacks begins with an attacker contacting its victim (e.g. via an email) urging them to visit a particular website (e.g. a spoofed version of a banking website), The spoofed website is constructed to persuade the victim in providing sensitive information.

For a phishing attack to succeed, the impersonation of a trusted party should be sufficiently convincing for the victim to believe they are interacting with the actual impersonated party. Therefore, phishers employ a range of techniques to increase their perceived trustworthiness.

The aforementioned

impersonation Phishing is one of the more prevalent and financially damaging computer attacks in place nowadays.

2 Methods and theory

3 Results

4 Discussion

The code can be found on GitHub[1].

[1] `https://github.com/kdhageman/phishing_generator`