Questions 02-19-2018

Malicious URL detection using machine learning: A survey:

This article discusses the research that has been conducted on applying machine learning algorithms to autonomous detection of malicious URLs. One of the challenges within the existing research resides in concept drift. We need machine learning algorithms that can consider concept drift in the form of new attack vectors and features in malicious URLs. Can we think of any ideas that may help with solving this issue? It seems, abstractly, that we need to apply machine learning within machine learning.

Discovering topological patterns in time-series big graph:

This article discusses topological pattern mining in big graphs. We have looked at intrusion detection and response systems that attempt to categorize the attack. This can be to take a specific action or just to classify the attack so that the system administrator can take a specific action. Can we use this topological pattern mining technique use big graphs to help categorize intrusions? Are there other uses for the methods and work presented in this paper in the realm of cyber security?