World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:09, 2022

Towards an Enhanced Compartmental Model for Profiling Malware Dynamics

Authors : Jessemyn Modiini, Timothy Lynar, Elena Sitnikova

Abstract : We present a novel enhanced compartmental model for malware spread analysis in cyber security. This paper applies cyber security data features to epidemiological compartmental models to model the infectious potential of malware. Compartmental models are most efficient for calculating the infectious potential of a disease. In this paper, we discuss and profile epidemiologically relevant data features from a Domain Name System (DNS) dataset. We then apply these features to epidemiological compartmental models to network traffic features. This paper demonstrates how epidemiological principles can be applied to the novel analysis of key cybersecurity behaviours and trends and provides insight into threat modelling above that of kill-chain analysis. In applying deterministic compartmental models to a cyber security use case, the authors analyse the deficiencies and provide an enhanced stochastic model for cyber epidemiology. This enhanced compartmental model (SUEICRN model) is contrasted with the traditional SEIR model to demonstrate its efficacy.

Keywords : cybersecurity, epidemiology, cyber epidemiology, malware
Conference Title : ICCP 2022 : International Conference on Cybersecurity and Privacy
Conference Location : Amsterdam, Netherlands
Conference Dates : September 15-16, 2022