THREAT PREDICTION BASED ON DNS TRAFFIC USER BEHAVIOUR WITH MACHINE LEARNING TECHNIQUES

A J C E Fernando

A dissertation submitted in partial fulfilment of the requirements for the

MSc in Cyber Security and Forensics Degree

Department of Computing

Informatics Institute of Technology, Sri Lanka

in Collaboration with

University of Westminster, UK

2021

Abstract

Cyber threats are more common in these days and plethora of attacks taking place daily worldwide. Most of these attacks are tributary to global economy, safety and compliance which can veer devastate the stability of the society. These attacks sustain due to lurking visibility or knowledge on the users, devices, information, application and networks within the environment. Therefore, Domain Name Service (DNS) based analysis mechanism is extremely suitable to address the current scenario with decisively Identify, Detect and Response mechanisms used in cyber resilience and execution. In this research, we build a method to predict the likelihood for the internet surfing users near real time cyber risk to an organization based on the DNS traffic. The machine learning (ML) techniques en-route the likelihood prediction which enlighten the conditions become more treacherous and focus on covert information from incident analyst. In this technique, an agent is used during the data collection phase to avoid the dependencies on Dynamic Host Configuration Protocol (DHCP) IP address lease, Enterprise Local Area Network (LAN) and user identification.

Keywords: *Domain Name Service, Machine Learning, Dynamic Host Configuration Protocol, Local Area Network.*