Politecnico di Torino

Finanziato dall'Unione europea
NextGenerationEU

COMPUTER AND CONTROL ENGINEERING

Automatic web threats identification via AI

Funded By	ERMES CYBER SECURITY SRL [P.iva/CF:11716270019] Ministero dell'Università e della Ricerca - MUR [P.iva/CF:96446770586]
Supervisor	MELLIA MARCO - marco.mellia@polito.it
Contact	MELLIA MARCO - marco.mellia@polito.it VASSIO LUCA - luca.vassio@polito.it
Context of the research activity	This scholarship focuses on the study, design and engeneering of automatic identification systems of cyber-attacks that adopt Social Engineering techniques. Phishing, Spear phishing, SMShing, Vishing, etc. they are all attacks that try to trick the user for stealing personal information or delivering malware. Thanks to the use of artificial intelligence-based methodologies such as Natural Language Processing, Reinforcement Learning, and supervised methodologies in general, we intend to create systems for the automatic identification of new attacks (zero-day threats) by creating data-driven, scalable, and automatic solutions.
Objectives	The purpose of this doctorate is to identify in general the traits that distinguish communications with malicious purposes, regardless of the channel used and the type of attack to be perpetrated. For this, it is essential to collect data and metadata that allow one identifying the characteristic features of the attack and trace the matrix to perform Threat Intelligence functions. The use of Machine Learning and Artificial Intelligence in general entails consequences that must be addressed with expertise. First of all, the application of classifiers based on supervised models mandates special attention in the case of cyber security. The strong imbalance that exists between benign and malicius cases must be taken into consideration from the early stages of the design to avoid running into performance issues that can prove problematic in real application scenarios (e.g. high frequency of false positives). Second, Machine Learning, and especially neural networks, introduce problems of interpretability of the results that are not acceptable in cyber security applications. It will therefore be necessary to pay particular attention to understanding how the solution works and which features of the data were decisive in the results. Finally, it will be necessary to address the problem of data scarcity and use tools for the generation of synthetic

	(possibly adversarial) data to strengthen the classifiers. The scholarship takes place in collaboration with the company Ermes Cyber Security SRL, an all-Italian company that has established itself as one of the most innovative in the fields of Artificial Intelligence and Cyber Security. Throughout the doctoral course, together with the company Ermes Cyber Security, we will pay great attention to measurement and data collections activities, both to collect useful data for the design of classifiers, and to quantify the pervasiveness of the threats faced.

Skills and competencies for the development of the activity	Advanced programming skills in C/C++, Java, Python. Solid knowledge in data mining techniques, machine learning and artificial intelligence approaches. Knowledge on cybersecurity for web applications is preferential.