Cross-Lingual Cybersecurity Analytics in the International Dark Web with Adversarial Deep Representation Learning

Mohammadreza Ebrahimi, Yidong Chai, Sagar Samtani, and Hsinchun Chen

Abstract

International dark web platforms operating within multiple geopolitical regions and languages host a myriad of hacker assets such as malware, hacking tools, hacking tutorials, and malicious source code. Cybersecurity analytics organizations employ machine learning models trained on human-labeled data to automatically detect these assets and bolster their situational awareness. However, the lack of human-labeled training data is prohibitive when analyzing foreign-language dark web content. In this research note, we adopt the computational design science paradigm to develop a novel IT artifact for cross-lingual hacker asset detection (CLHAD). CLHAD automatically leverages the knowledge learned from English content to detect hacker assets in non-English dark web platforms. CLHAD encompasses a novel adversarial deep representation learning (ADREL) method, which generates multilingual text representations using generative adversarial networks (GANs). Drawing upon the state of the art in cross-lingual knowledge transfer, ADREL is a novel approach to automatically extract transferable text representations and facilitate the analysis of multilingual content. We evaluate CLHAD on Russian, French, and Italian dark web platforms and demonstrate its practical utility in hacker asset profiling, and conduct a proof-of-concept case study. Our analysis suggests that cybersecurity managers may benefit more from focusing on Russian to identify sophisticated hacking assets. In contrast, financial hacker assets are scattered among several dominant dark web languages. Managerial insights for security managers are discussed at operational and strategic levels.

Keywords: Cybersecurity analytics, dark web, automated hacker asset detection, cross-lingual knowledge transfer, adversarial learning, computational design science