APT attack detection based on Threat Hunting and a specific case study on 1937CN

Nguyen Tuan Anh

Abstract: This topic proposes a method for detecting APT (Advanced Persistent Threat) attacks through Threat Hunting techniques, aiming to address the increasingly sophisticated state of cyber espionage attacks. The objective of the research is to build a system for automatic recognition and response to suspicious activities in corporate network environments. The method combines Threat Hunting theory with experimentation to implement a specific case study related to 1937CN, with the goal of providing an effective security solution and contributing to the field of information security research.

Keywords: Threat Hunting, APT, Case Study, Cybersecurity, Security