Ministry of Higher Education and
Scientific Research
University of Babylon
College of Information Technology
Department of Information Security
Study: (Morning)

Detection Malware

Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the A Graduate Project Submitted to the department of Requirements for the Bachelor's degree in the Information Security of Information Technology

By Students

Esraa Ghaleb Abd

Supervised by

Assist.lect.Noha Kareem

Babylon, Iraq

2024 - 2023

Abstract

The lecture discusses the persistent threat of malware to computer systems and networks, highlighting the challenges it poses to cybersecurity professionals. It emphasizes the need for intelligent tools to analyze, classify, and detect malware efficiently. Traditional signature-based methods are effective against known malware but struggle with zero-day threats and polymorphic variants. In contrast, machine learning offers promise in detecting unseen malware by learning patterns and behaviors. The proposed hybrid approach combines both techniques, leveraging signature-based detection for known malware and machine learning for zero-day threats. Key aspects include feature fusion, ensemble methods, and a feedback loop mechanism for continuous improvement. Experimental results demonstrate high detection rates with minimal false positives, providing comprehensive protection against evolving malware threats. Overall, the approach offers a practical and effective solution for malware detection in modern computing environments by leveraging the complementary strengths of machine learning and signature-based techniques.

.