الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 5491 - سيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbes

Mémoire

En vue de l'obtention du diplôme de **Master**

Domaine : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques**

Thème

Analyse Systémique des Méthodologies d'Intelligence Artificielle pour la Détection des Ransomwares

---

Présenté par
Kebbas Mohammed Houssameddine

Soutenu le : **01 octobre 2025**
Devant le jury composé de

Dr. KHALDI Miloud	Président du jury
Dr. BENDELLA Mohammed Salih	Encadreur
Dr. BENSENANE Hamdane	Co-encadreur
Dr. BABA-AHMED Manel	Examinatrice

Année universitaire : 2024/2025

Résumé

Les ransomwares représentent une menace de cybersécurité majeure et en constante évolution, rendant les méthodes de détection traditionnelles basées sur les signatures largement obsolètes. Ce mémoire aborde la problématique de la détection des ransomwares en explorant le potentiel des techniques d'intelligence artificielle (IA), notamment l'apprentissage automatique (Machine Learning) et l'apprentissage profond (Deep Learning).

Ce travail propose une étude approfondie de l'écosystème des ransomwares, incluant leurs stratégies d'attaque, leurs mécanismes techniques et leurs modèles économiques. Nous présentons ensuite une revue des outils et des méthodologies d'analyse — statique et dynamique — qui permettent d'extraire des caractéristiques pertinentes du comportement des malwares.

Le cœur de ce mémoire réside dans un état de l'art détaillé de la recherche scientifique actuelle. Nous y analysons et comparons plusieurs approches de détection de pointe, allant des systèmes d'analyse comportementale à grande échelle aux modèles de Deep Learning capables de s'adapter en continu aux nouvelles menaces. L'analyse couvre des contextes variés, tels que la détection de menaces évasives, la protection des infrastructures cloud et la détection à très faible latence au niveau du noyau système.

En conclusion, ce travail de synthèse met en évidence les tendances actuelles de la recherche, souligne la suprématie de l'analyse comportementale et le rôle central de l'IA, et identifie les défis et les perspectives pour le développement de solutions de détection de ransomwares plus robustes, adaptatives et contextuelles.

Mots-clés : Ransomware, Détection de malwares, Intelligence Artificielle, Apprentissage Automatique, Apprentissage Profond, Analyse Statique, Analyse Dynamique.

Abstract

Ransomware represents a major and constantly evolving cybersecurity threat, rendering traditional signature-based detection methods largely obsolete. This thesis addresses the issue of ransomware detection by exploring the potential of Artificial Intelligence (AI) techniques, particularly Machine Learning and Deep Learning.

This work provides a comprehensive study of the ransomware ecosystem, including its attack strategies, technical mechanisms, and economic models. We then present a review of the fundamental analysis tools and methodologies—static and dynamic—used to extract relevant features from malware behavior.

The core of this thesis lies in a detailed state-of-the-art review of current scientific research. We analyze and compare several cutting-edge detection approaches, covering diverse contexts such as detecting evasive threats, protecting cloud infrastructures, and achieving very low-latency detection at the operating system kernel level.

Furthermore, this thesis conducts a comparative and critical analysis of these methodologies. It delves into the fundamental trade-offs between detection speed, precision, and robustness. The challenges inherent to AI-based systems, such as the need for high-quality datasets, adaptability against zero-day threats, and the vulnerability to adversarial attacks, are also thoroughly discussed.

In conclusion, this synthesis identifies current research trends, emphasizes the supremacy of behavioral analysis and the central role of AI, and outlines key challenges and future directions for the development of more robust, adaptive, and context-aware ransomware detection solutions.

Keywords : Ransomware, Malware Detection, Artificial Intelligence, Machine Learning, Deep Learning, Static Analysis, Dynamic Analysis, Cybersecurity.

ملخص

تمثل برامج الفدية تهديدًا كبيرًا ومتطورًا في مجال الأمن السيبراني، مما يجعل طرق الكشف التقليدية المعتمدة على التوقيعات الرقمية غير فعالة إلى حد كبير. تتناول هذه المذكرة إشكالية الكشف عن برامج الفدية من خلال استكشاف إمكانيات تقنيات الذكاء الاصطناعي، وبالأخص تعلم الآلة والتعلم العميق.

يقدم هذا العمل دراسة معمقة لمنظومة برامج الفدية، بما في ذلك استراتيجيات الهجوم، الآليات التقنية، والنماذج الاقتصادية. كما نستعرض الأدوات والمنهجيات التحليلية — الساكنة والديناميكية — المستخدمة لاستخلاص السمات السلوكية للبرمجيات الخبيثة.

يكمن جوهر هذه المذكرة في تقديم عرض مفصل لأحدث ما توصل إليه البحث العلمي في هذا المجال. حيث نحلل ونقارن بين عدة مناهج كشف متقدمة، تغطي سياقات متنوعة مثل كشف التهديدات المراوغة، حماية البنى التحتية السحابية، والكشف بزمن استجابة منخفض على مستوى نواة النظام.

في الختام، تلخص هذه الدراسة الاتجاهات البحثية الحالية، وتؤكد على هيمنة التحليل السلوكي والدور المركزي للذكاء الاصطناعي، كما تحدد التحديات والآفاق المستقبلية لتطوير حلول كشف لبرامج الفدية تكون أكثر قوة ومرونة وتكيفًا مع السياق.

كلمات مفتاحية : برامج الفدية، الكشف عن البرمجيات الخبيثة، الذكاء الاصطناعي، تعلم الآلة، التعلم العميق، التحليل الساكن، التحليل الديناميكي .