الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 08 ماي 5491 بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **Master**
Field: **Computer Science**
Specialty: **Ingénierie des Systèmes Informatiques (ISI)**

Theme

XAI-powered Sophisticated Malware Detection: a comparative study

---

Presented by:
Rezkallah Razene
Benmaissa Sarah

Submission Date: **Oct, 2024**
In front of the jury composed of:

Pr. AMAR BENSABER Djamel	President
Dr. AMRANE Abdelkader	Supervisor
Mr. FECHFOUCH Mostafa	Co-Supervisor
Dr. BEDJAOUI Mohammed	Examinator

Academic Year : 2023/2024

Abstract

With the use of defending mechanisms and vulnerability detection tools, malwares sometimes find their way to the computers causing big damage, which affects large services and organizations. With the constant rise of malware threats, malware detection plays an indispensable role in protecting information systems. As attacking techniques evolve, traditional malware detection approaches (based on signatures, network packets, etc.) are no longer efficient with sophisticated malwares. This research contributes to advancing the field of malware detection and combating evolving cyber threats, with the utilization of memory forensics techniques from CIC-MalMem-2022 dataset coupled with machine learning algorithms and XAI (Explainable Ai) to enhance fileless and obfuscated malware detection and classification with advanced approaches.

Keywords— Cybersecurity, Malwares, Threats, Memory Forensics, Artificial Intelligence (AI), Machine Learning (ML), Explainable AI (XAI)

الملخص

مع استخدام آليات الدفاع وأدوات الكشف عن الثغرات، تتمكن البرمجيات الخبيثة أحيانًا من الوصول إلى أجهزة الحواسيب متسببة في أضرار كبيرة تؤثر على خدمات ومؤسسات واسعة النطاق. ومع الزيادة المستمرة في تهديدات البرمجيات الخبيثة، يلعب الكشف عن البرمجيات الخبيثة دورًا لا غنى عنه في حماية أنظمة المعلومات. ومع تطور تقنيات الهجوم، أصبحت أساليب الكشف التقليدية (المعتمدة على التوقيعات، حزم الشبكة، إلخ) غير فعّالة مع البرمجيات الخبيثة المتطورة.

يساهم هذا البحث في تقدم مجال اكتشاف البرمجيات الخبيثة ومكافحة التهديدات الإلكترونية المتطورة من خلال استخدام تقنيات فحص الذاكرة من مجموعة بيانات CIC-MalMem-2022، إلى جانب خوارزميات التعلم الآلي والذكاء الاصطناعي القابل للتفسير (XAI)، لتعزيز الكشف عن البرمجيات الخبيثة بدون ملفات والمموهة وتصنيفها باستخدام أساليب متقدمة.

الكلمات المفتاحية — الأمن السيبراني، البرمجيات الخبيثة، التهديدات، فحص الذاكرة، الذكاء الاصطناعي (AI)، التعلم الآلي، الذكاء الاصطناعي القابل للتفسير (XAI).

Résumé

Avec l'utilisation de mécanismes de défense et d'outils de détection des vulnérabilités, les malwares parviennent parfois à infiltrer les ordinateurs, causant d'importants dégâts qui affectent de grands services et organisations. Avec la montée constante des menaces de malwares, la détection des malwares joue un rôle indispensable dans la protection des systèmes d'information. À mesure que les techniques d'attaque évoluent, les approches traditionnelles de détection des malwares (basées sur les signatures, les paquets réseau, etc.) ne sont plus efficaces face aux malwares sophistiqués.

Cette recherche contribue à l'avancement du domaine de la détection des malwares et à la lutte contre les menaces cybernétiques évolutives grâce à l'utilisation des techniques de mémoire forensique issues du dataset CIC-MalMem-2022, couplées à des algorithmes d'apprentissage automatique et à l'Intelligence Artificielle Explicable (XAI), pour améliorer la détection et la classification des malwares obfusqués et sans fichier à l'aide d'approches avancées.

Mots-clés — Cybersécurité, Malwares, Menaces, Mémoire Forensique, Intelligence Artificielle (IA), Apprentissage Automatique, Intelligence Artificielle Explicable (XAI).
