УДК 004.056

РАЗРАБОТКА МЕТОДИКИ ОБНАРУЖЕНИЯ БЕСФАЙЛОВОГО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ПАМЯТНОЙ ФОРЕНЗИКИ И МАШИННОГО ОБУЧЕНИЯ

Нгуен Х.Х.
Научный руководитель – канд. техн. наук, доцент Канжелев Юрий Алексеевич
Университет ИТМО
Anhhiep04082000@gmail.com

Введение

В современных условиях кибербезопасности бесфайловое вредоносное программное обеспечение (ПО) представляет собой одну из наиболее серьезных угроз, так как оно функционирует исключительно в оперативной памяти, обходя традиционные средства защиты, ориентированные на анализ файлов. Традиционные антивирусные средства защиты зачастую оказываются неэффективными против таких атак, как Process Hollowing или Reflective DLL Injection, из-за отсутствия последних версий сигнатур на диске. В связи с этим, актуальной задачей является разработка методик, объединяющих возможности памятной форензики для извлечения скрытых артефактов и алгоритмов машинного обучения для автоматизации процесса классификации и обнаружения аномалий. Данная работа направлена на создание комплексного подхода к выявлению бесфайлового вредоносного ПО, обеспечивающего высокую точность и оперативность реагирования на инциденты.

Основная часть

Предлагаемый подход базируется на переходе от традиционного сканирования файлов к исследованию оперативной памяти, что позволяет обнаруживать скрытые угрозы, не оставляющие следов на физических носителях. В основе данного решения лежит реализация комплексной пятифазной архитектуры, объединяющей памятную форензику с использованием фреймворка Volatility для извлечения артефактов и автоматизированную классификацию на базе алгоритмов машинного обучения [1, 2, 3]. Технологическое преимущество обеспечивается за счет интеграции с облачной экосистемой Amazon Web Services, где использование бессерверных функций и масштабируемых хранилищ позволяет эффективно обрабатывать массивы данных без необходимости содержания дорогостоящих локальных серверов. Применение специализированного набора данных, ориентированного на обфусцированное вредоносное ПО, адаптирует систему к выявлению наиболее замаскированных современных кибератак.

Выводы

Проведенные исследования подтверждают, что сочетание методов памятной форензики и алгоритмов машинного обучения является эффективным решением для обнаружения бесфайлового вредоносного ПО, которое успешно обходит традиционные средства защиты. Разработанный автоматизированный подход позволяет не только выявлять скрытые угрозы в оперативной памяти с высокой точностью, но и значительно сокращать время реагирования на инциденты. Использование облачной инфраструктуры обеспечивает необходимую масштабируемость для анализа больших объемов данных, делая систему пригодной для использования в реальных корпоративных средах.

Список использованных источников:

1. An Insight into the Machine-Learning-Based Fileless Malware Detection. Sensors 2023. URL: https://www.mdpi.com/1424-8220/23/2/612 (дата обращения: 08.01.2026).
2. RAM Forensics: The Analysis and Extraction of Malicious Processes from Memory Image Using GUI Based Memory Forensic Toolkit. URL: https://doi.org/10.1109/ICCUBEA.2018.8697752 (дата обращения: 11.01.2026).
3. Michael H. L., Andrew C., Jamie L., AAron Walters. Art of Memory Forensics.

Обучающийся _____ Нгуен Хоанг Хиеп
(Фамилия И.О.)

Научный руководитель _____ Канжелев Юрий Алексеевич
(Фамилия И.О.)