УДК 004.8

Кулешов Арсений Алексеевич

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ И БЛОКИРОВКИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ АНАЛИЗА ИЗОБРАЖЕНИЙ И КОМПЬЮТЕРНОГО ЗРЕНИЯ

В данной работе предлагается методика обнаружения и блокировки вредоносного программного обеспечения (ВПО) с использованием анализа изображений и компьютерного зрения. Этот подход позволяет эффективно выявлять и предотвращать атаки, основанные на новых методах скрытия и обхода традиционных средств защиты. Система основана на использовании алгоритмов машинного обучения для анализа визуальных данных, полученных от пользователей или сетевого трафика. Предложенный подход может быть успешно применен для защиты информационных систем в различных сферах, включая корпоративную сетевую безопасность, киберзащиту критической инфраструктуры и защиту персональных данных.

Вредоносное программное обеспечение, обнаружение угроз, компьютерное зрение, анализ изображений, системы безопасности, машинное обучение, кибербезопасность, защита информации, атаки на ПО, сетевая безопасность.

Kuleshov Arseny Alexeevich

DEVELOPMENT OF A SYSTEM FOR DETECTING AND BLOCKING MALICIOUS SOFTWARE USING IMAGE ANALYSIS AND COMPUTER VISION

A methodology for detecting and blocking malicious software (malware) using image analysis and computer vision is proposed. This approach enables efficient detection and prevention of attacks based on new evasion and obfuscation techniques. The system relies on machine learning algorithms to analyze visual data obtained from users or network traffic. The proposed approach can be successfully applied to protect information systems in various domains, including corporate network security, critical infrastructure cybersecurity, and personal data protection.

Malicious software detection, image analysis, computer vision, efficiency analysis, cybersecurity, threat detection, machine learning, anomaly detection, pattern recognition, cyber threat mitigation.

Введение

Тема создания системы обнаружения и блокировки вредоносного программного обеспечения (ВПО) с использованием анализа изображений и компьютерного зрения находится в центре внимания в связи с постоянным увеличением числа киберугроз и развитием новых методов атак. Актуальность этой темы обусловлена необходимостью разработки эффективных инструментов для борьбы с различными видами вредоносного ПО, включая вирусы, троянские программы, шпионские модули и другие угрозы, которые могут причинить серьезный ущерб информационной безопасности организаций и частных лиц.

Использование анализа изображений и компьютерного зрения для обнаружения вредоносного ПО представляет собой инновационный подход, который позволяет выявлять новые угрозы и атаки, основываясь на визуальных данных, полученных от пользователя или из других источников. Данный подход позволяет обнаруживать вредоносное ПО, которое может быть скрыто в обычном трафике или обходит традиционные методы обнаружения, такие как сигнатурные анализаторы или системы предупреждения об инцидентах.

Разработка и внедрение системы обнаружения и блокировки ВПО на основе анализа изображений и компьютерного зрения требует совместной работы специалистов по информационной безопасности, специалистов по машинному обучению и компьютерному зрению, а также разработчиков программного обеспечения. Такие системы могут быть применены в различных сферах, включая корпоративную информационную безопасность, киберзащиту критической инфраструктуры, защиту персональных данных и другие области, где важна защита от киберугроз.

Основная часть

Система обнаружения и блокировки вредоносного программного обеспечения (ВПО) с использованием анализа изображений и компьютерного зрения представляет собой инновационный подход к борьбе с киберугрозами, который объединяет в себе передовые методы анализа данных и технологии искусственного интеллекта.

Ключевой идеей данной системы является использование изображений, получаемых из сети Интернет, в ходе коммуникации между пользователями ИС или из других источников, для выявления потенциально вредоносного ПО в результате фонового анализа. Для реализации данной задачи используются следующие технологии ИБ:

1. Обнаружение аномалий, с помощью которых система может анализировать изображения на наличие аномальных или подозрительных элементов, таких как неизвестные программные интерфейсы, артефакты или нетипичные структуры данных, которые могут указывать на наличие вредоносного программного обеспечения [5].

2. Классификация объектов, с помощью которой методами машинного обучения система может определять характеристики и формы объектов на изображении и сравнивать их с базой данных известных вредоносных элементов.

3. Сегментация изображений, для которой используются техники сегментации изображений в целях выделения отдельных объектов или областей на изображении, что позволяет более точно анализировать их структуру и содержание.

4. Поведенческий анализ, то есть анализ временных рядов и динамики изменений в изображениях для выявления аномальных паттернов и поведения, которые могут свидетельствовать о наличии вредоносного ПО [4].

5. Блокировка при обнаружении подозрительных элементов или активностей, а также меры по блокировке или исключению вредоносного ПО

Эффективность такой системы обнаружения вредоносного программного обеспечения может быть значительно увеличена за счет комбинации различных методов анализа изображений и компьютерного зрения с передовыми технологиями искусственного интеллекта и машинного обучения. Кроме того, важным аспектом является постоянное обновление системы и базы данных для обеспечения ее актуальности и эффективности в поиске и блокировке новых угроз.

Существующие методы обнаружения и блокировки ВПО имеют ряд недостатков, включая низкую скорость реакции на новые угрозы, сложность адаптации к разнообразным типам ВПО и неэффективность в обнаружении скрытых угроз и уязвимостей «нулевого дня». Это создает потребность в разработке новых подходов, способных обеспечить более высокий уровень защиты.

Кроме вышеперечисленных методов анализа, система также может использовать различные техники и подходы для обнаружения вредоносного программного обеспечения на основе изображений. Например, одним из методов может быть анализ текстур и цветовых характеристик изображений. Вредоносное ПО часто имеет определенные текстурные или цветовые особенности, которые могут быть обнаружены с помощью алгоритмов анализа изображений. Это может включать в себя поиск аномальных участков с необычными текстурами или цветовыми схемами, которые отличаются от типичных шаблонов в безопасных программах.

Примером может служить обнаружение вредоносных файлов внутри архивов. Система анализирует изображения содержимого архивов и может выявлять подозрительные элементы, такие как аномальные текстуры или цвета в файловых структурах. Например, если вредоносный файл содержит скрытые данные или вредоносный код, который не обнаруживается традиционными методами сканирования, система может использовать анализ изображений для выявления таких аномалий и предпринимать соответствующих мер по блокировке или удалению угрозы.

Еще одним примером может быть анализ цифровых подписей и стеганографии в изображениях. Вредоносные программы могут использовать различные методы для скрытия своего кода или данных внутри изображений, используя цифровые подписи или стеганографию. Система обнаружения и блокировки ВПО может проводить анализ цифровых подписей и стеганографических методов, чтобы выявлять скрытые угрозы и предотвращать их воздействие на систему.

В рамках данной работы реализована система анализа изображений на наличие вредоносов, основанная на машинном обучении. Нейронная сеть производит анализ по паттернам, представленным на входных изображениях, и, исходя из баз однозначно вредоносных изображений и характерных им паттернов, делает вывод, заражено ли изображение или нет.

Данный подход возможен благодаря заранее подготовленному dataset вредоносных изображений, на котором описанная в данной работе нейронная сеть прошла обучение в рамках 10 эпох.

Преимуществом данной системы является более глубокий анализ по сравнению с вышеуказанными уже существующими средствами.

Обобщенная архитектура программной реализации представлена на рис. 1.

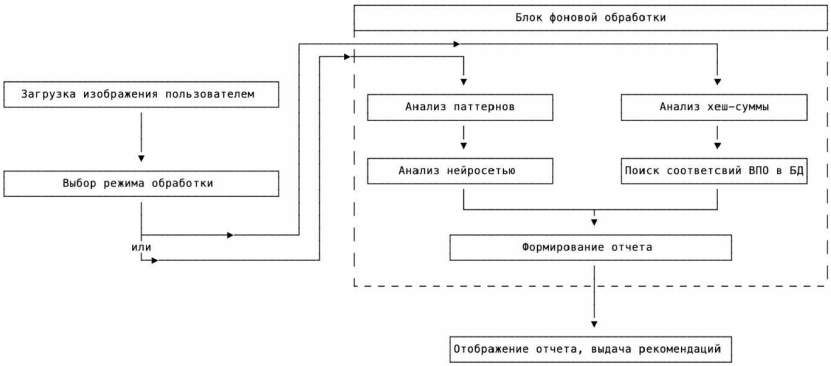

Рис. 1. Обобщенная архитектура ПО

Ниже представлен веб-интерфейс реализованного средства в процессе анализа (рис. 2) и с уже полученным результатом, дополненным показателем выявления вредоносов в загруженной картинке в процентах (рис. 3).

Наиболее известным и технически продвинутым на нынешний момент средством поиска вредоносных изображений является антивирусное программное обеспечение [6].

Рис. 2. Процесс анализа

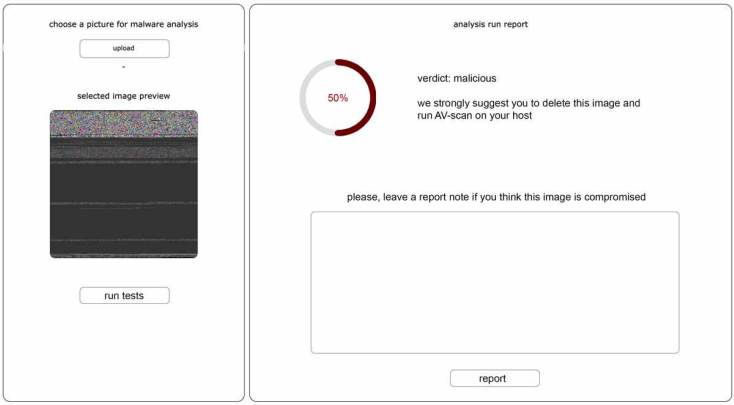

Рис. 3. Отображение результата анализа

АВПО является комплексным решением для защиты ЭВМ от ВПО, и чаще всего основано на сигнатурном анализе. Это означает, что при выполнении планового сканирования средством АВПО происходит вычисление хеш-сумм файлов, размещенных на хосте, и сопоставление полученных хеш-сумм с базой сигнатур. Если найдено соответствие, ПО классифицируется и как вредоносное, и АВПО принимает меры по нейтрализации угрозы.

Реализованное в рамках данной работы программное средство имеет ряд преимуществ перед уже существующими АВПО, некоторые из которых включают: глубокий анализ с учетом зафиксированных ранее атак и попыток эксплуатации уязвимостей ОС с помощью вредоносных изображений с помощью обнаружения паттернов, а не на основе сигнатурного анализа по хеш-функции, также, данная реализация способна сформировать рекомендации по нейтрализации угрозы для пользователя исходя из оценки вредоносности проанализированного изображения.

Таким образом, пользователь, загрузив подозрительное изображение на указанный выше ресурс, имеет возможность получить информацию, стоит ли удалять данное изображение, или оно не является опасным. В случае, если изображение действительно представляет угрозу, представленный в данной работе ресурс сообщит это пользователю, указав в качестве рекомендации провести полную проверку хостовым СЗИ.

Выводы

Разработка системы обнаружения и блокировки ВПО с использованием анализа изображений и компьютерного зрения представляет собой важный шаг в обеспечении кибербезопасности. Ее применение может значительно снизить риск инцидентов безопасности и повысить уровень защиты информационных ресурсов. Дальнейшее исследование и развитие этой технологии позволит обеспечить еще более надежную защиту в условиях постоянно меняющейся киберугрозовой обстановки.

Данная технология потенциально представляет большой интерес для корпораций различного масштаба, так как ее внедрение может обеспечить усиленную безопасность при работе с информацией, составляющей коммерческую тайну.

В целом, предложенное в данной работе программное решение на основе машинного обучения может составить конкуренцию существующим средствам обнаружения ВПО. Тем не менее, для дальнейшего развития средства анализа наличия вредоносов в изображениях потребуются дальнейшие доработки, обучение нейронных сетей и сравнительно большие мощности ЭВМ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Панарин В. М., Гришаков К. В., Маслова А. А., Гришакова О. В., Архипов А. В. и др.* Нейроны в нейронных сетях // Известия ТулГУ. Технические науки. 2023. № 2.

2. *Зрелова Д. П., Ульянов С. В.* Модели физически информированных / осведомленных классических лагранжевых / гамильтоновых нейронных сетей в глубоком обучении // Современные информационные технологии и ИТ-образование. 2022. № 2.

3. *Сторожок Е. А., Дорофеев Г. В., Стародубцев П. А.* Классификация сигналов с использованием технологии нейронных сетей // Журнал СФУ. Техника и технологии. 2022. № 3.

4. *Филюков Д. А.* Применение нейронных сетей для формирования кода вредоносного программного обеспечения // Инновации и инвестиции. 2023. № 7.

5. *Лихотин М. А.* Использование свёрточных нейронных сетей для анализа изображений // Вестник ВГТУ. 2023. № 2.

6. *Павликов С. Н., Коломеец В. Ю., Колесов Ю. Ю., Петров П. Н., Афанасьев Р. К.* Метод обнаружения вредоносных программ и их элементов // Наукоемкие технологии в космических исследованиях Земли. 2022. № 3.

7. *Латыпова Д. С., Тумаков Д. Н.* Применение технологии CUDA для обучения нейронной сети Кохонена // Программные продукты и системы. 2022. № 3.

8. *Карпов К. Д., Холмогоров В. В.* Система оценки качества изображения на основе компьютерного зрения // International Journal of Open Information Technologies. 2022. № 12.

9. *Айткенова М. К., Сарсенбаева Ж., Сартбасов Б. Б.* Виды вредоносного программного обеспечения // НИР/S&R. 2022. № 2 (10).

10. *Дрюченко М. А., Сирота А. А.* Стегоанализ цифровых изображений с использованием глубоких нейронных сетей и гетероассоциативных интегральных преобразований // ПДМ. 2022. № 55.

Кулешов Арсений Алексеевич, студент Донского Государственного Технического Университета, Россия, город Ростов-на-Дону, пл. Гагарина, 1, 344000, телефон: +7 (928) 129-45-30, email: arseniykul@gmail.com.

Kuleshov Arseny Alekseevich, student of Don State Technical University, Russian Federation, Rostov-on-Don, Gagarina sq., 1, 344000, phone: +7 (928) 129-45-30, email: arseniykul@gmail.com.