Разработка системы анализа файлов с элементами искусственного интеллекта

П.А. Серов, С.С. Иванов, Г.В. Скляр

Филиал Самарского государственного технического университета, Сызрань, Россия

Обоснование. В современном бизнесе многие организации становятся мишенями различных атак, включая те, которые используют вредоносное программное обеспечение. Основные каналы распространения таких угроз — это электронная почта и веб-трафик. Из-за высокого уровня риска при получении файлов из внешних источников компаниям необходимы разнообразные средства защиты. Выбор конкретных защитных решений во многом зависит от типа деятельности компании, методов ее коммуникации и ее размеров. Если в компании используется удаленный доступ к инфраструктуре, то ей нужно обеспечить безопасность ресурсов, к которым осуществляется доступ [1]. Если взаимодействие с подрядчиками и клиентами осуществляется через электронную почту, компании необходима программа, обеспечивающая безопасность почтовых шлюзов, и проверка входящего трафика. Существуют различные виды атак, которым может подвергнуться инфраструктура бизнеса в случае отсутствия защиты почтовых шлюзов.

Даже при наличии защитного программного обеспечения добиться полного уровня защиты инфраструктуры довольно сложно, поскольку риски могут возникать и от самих поставщиков таких решений. Песочницы представляют собой защитное программное обеспечение, которое создает изолированную виртуальную среду для запуска файлов и анализа их поведения. Это помогает предотвратить возможный ущерб основной операционной системе или данным, если программа окажется вредоносной [2, 3]. В контексте кибербезопасности «песочница» представляет собой строго контролируемую среду, где можно безопасно выполнять подозрительные программы или скрипты. Однако файлы могут передаваться на анализ к поставщику, что в свою очередь создает дополнительные риски: если злоумышленник сможет получить доступ к инфраструктуре подрядчика и нарушит цепочку поставок, существует вероятность, что он получит доступ к инфраструктуре и/или данным клиентов подрядчика.

Цель — создание системы для анализа файлов с применением элементов искусственного интеллекта.

Методы. Современные песочницы способны в реальном времени отслеживать подозрительное поведение файлов, включая поведенческий анализ. Поведенческий анализ в рамках песочницы представляет собой метод мониторинга действий файла в изолированной виртуальной среде. Эффекты работы файла оцениваются на основе его действий в этой обстановке. Песочница может фиксировать различные подозрительные действия, такие как запросы на загрузку или отправку данных на внешний сервер, а также попытки установить дополнительные модули или компоненты.

Результаты. Чтобы снизить риски для компании, было решено разработать песочницу с базами данных, размещенными внутри инфраструктуры заказчика, что устраняет возможность доступа злоумышленников через цепочку поставок от поставщика песочницы. Также было принято решение создать опциональный модуль искусственного интеллекта, который способен сокращать количество ложных срабатываний и повышать точность анализа, обращаясь к информации о файлах в открытых источниках с помощью метода «паука».

К преимуществам новой песочницы, помимо наличия модуля ИИ и размещения внутри корпоративной инфраструктуры, относится ее способность имитировать реальную систему. Вредоносные файлы, основываясь на определенных сигнатурах и данных в системе (например, данных реестра или MAC-адресе), могут осознавать, что находятся в песочнице, и не проявлять вредоносную или подозрительную активность, что помогает избежать их обнаружения. Предлагаемое решение может манипулировать этими данными, что лишает вредоносные файлы одного из основных преимуществ. Дополнительно полезен как автоматический режим проверки, так и «ручной», позволяющий пользователю самостоятельно подключаться к системе, загружать файл и проверять его поведение.

Выводы. Размещение песочницы и баз данных внутри корпоративной инфраструктуры, наличие модуля ИИ и возможность имитации реальных данных помогают снизить количество ложных срабатываний при анализе файлов, а также минимизируют общий уровень риска компрометации данных в компании.

Ключевые слова: песочница; система анализа данных; поведенческий анализ; индикаторы компрометации; программное обеспечение; искусственный интеллект.

Список литературы

1. Серов П.А., Панов Д.А., Иванов С.С. Автоматизированное детектирование DDOS-атак // Сборник трудов VI Всероссийской научно-практической конференции студентов и молодых ученых: «Молодежная наука: вызовы и перспективы». Самара, 2023. С. 218–220. EDN: FBGASF
2. Серов П.А., Панов Д.А., Иванов С.С., Садова К.В. Разработка IDS-системы на основе технологии множественных временных окон // XLIX Самарская областная студенческая научная конференция: сборник тезисов докладов. Санкт-Петербург, 2023. С. 396–397. EDN: OBFMWM
3. Серов П.А., Панов Д.А., Садова К.В. Обнаружение DDOS-атак на основе анализа сетевого трафика // Сборник трудов V Всероссийской научно-практической конференции студентов и молодых ученых: «Молодежная наука: вызовы и перспективы». Самара, 2022. С. 189–191. EDN: WFZATM

Сведения об авторах:

Павел Александрович Серов — студент, группа ЭИЗ-24; Филиал Самарского государственного технического университета, Сызрань, Россия. E-mail: serov.archer@gmail.com

Сергей Сергеевич Иванов — студент, группа ЭИЗ-24; Филиал Самарского государственного технического университета, Сызрань, Россия. E-mail: teamparker17@gmail.com

Глеб Валерьевич Скляр — студент, группа ЭИЗ-24; Филиал Самарского государственного технического университета, Сызрань, Россия. E-mail: sklyar.glebv@gmail.com

Сведения о научном руководителе:

Кристина Владимировна Садова — старший преподаватель кафедры «Информатика и системы управления»; Филиал Самарского государственного технического университета, Сызрань, Россия. E-mail: crazyojj@mail.ru