Система оценки файла на наличие вредоносного содержимого

П.А. Серов, С.С. Иванов, Г.В. Скляр

Филиал Самарского государственного технического университета, Сызрань, Россия

Обоснование. Множество организаций становятся жертвами различных атак, включая те, которые используют вредоносное программное обеспечение. Наиболее распространенные угрозы поступают через электронную почту и веб-трафик. В связи с высоким уровнем риска, связанным с получением файлов из внешних источников, компаниям необходимо применять разнообразные меры защиты [1]. 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, а 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. К примеру, пользователь может загрузить вредоносное ПО под предлогом легитимного письма или файла, что может привести к компрометации инфраструктуры, включая конфиденциальные данные и иную информацию [2, 3]. Даже с установленным защитным программным обеспечением достичь полного уровня защиты инфраструктуры довольно сложно, так как риски могут возникать и от самих поставщиков таких решений. Песочницы представляют собой защитные инструменты, создающие изолированную виртуальную среду для запуска файлов и анализа их поведения, что помогает предотвратить возможный ущерб основной операционной системе или данным в случае, если программа окажется вредоносной. В кибербезопасности «песочница» — это контролируемая среда, где можно безопасно выполнять подозрительные программы или скрипты. Однако передача файлов на анализ поставщику создает дополнительные риски: если злоумышленник получит доступ к инфраструктуре подрядчика и нарушит цепочку поставок, он может получить доступ к инфраструктуре и/или данным клиентов.

Цель — создание системы оценки файлов на наличие вредоносного содержимого с использованием элементов искусственного интеллекта.

Методы. В качестве метода мониторинга был использован поведенческий анализ, с помощью которого можно в реальном времени отслеживать подозрительное поведение файлов, фиксировать различные подозрительные действия, такие как запросы на загрузку или отправку данных на внешний сервер, а также попытки установки дополнительных модулей.

Результаты. Для снижения рисков было решено разработать песочницу с базами данных, размещенными внутри инфраструктуры заказчика, что исключает возможность доступа злоумышленников через компрометацию цепочки поставок. Также в работу был принят вариант создания опционального модуля искусственного интеллекта, который сокращает количество ложных срабатываний и повышает точность анализа, используя информацию о файлах из открытых источников с помощью метода «паука».

Преимущества новой песочницы включают наличие модуля ИИ и размещение внутри корпоративной инфраструктуры, а также способность имитировать реальную систему. Вредоносные файлы могут осознавать, что находятся в песочнице, и не проявлять вредоносную активность, что помогает избежать их обнаружения. Наша песочница может манипулировать данными, лишая вредоносные файлы одного из основных преимуществ. Также доступны как автоматический, так и «ручной» режим проверки, позволяющий пользователю загружать файл и проверять его поведение.

Выводы. Размещение песочницы и баз данных внутри корпоративной инфраструктуры, наличие модуля ИИ и возможность имитации реальной системы способствуют снижению количества ложных срабатываний при анализе файлов и минимизируют общий уровень риска компрометации данных в компании. Это позволяет более эффективно защищать инфраструктуру и данные от потенциальных угроз.

Ключевые слова: система оценки файла; песочница; поведенческий анализ; индикаторы компрометации; вредоносное программное обеспечение.

Список литературы

1. Серов П.А., Панов Д.А., Иванов С.С. Автоматизированное детектирование DDOS-атак // Сборник 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 // Сборник тезисов докладов XLIX Самарской областной студенческой научной конференции. 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 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