УДК 004.056.5

МЕТОДИКА ОБНАРУЖЕНИЯ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ЧЕРЕЗ ПРИЛОЖЕНИЯ ДЛЯ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

Давыдов М.А.

Научный руководитель – канд. техн. наук, доцент ФБИТ Югансон А.Н.

Университет ИТМО

mark.davydov.1024@gmail.com

Работа выполнена в рамках темы НИР №4 «Разработка методики обнаружения утечек конфиденциальной информации через приложения для обмена мгновенными сообщениями».

Введение

Рост использования мессенджеров в корпоративной среде повышает вероятность несанкционированной передачи данных: в переписке легко переслать фрагменты документов, персональные сведения или материалы, представляющие ценность для организации. Основная проблема состоит в том, что современный обмен сообщениями в веб-клиентах мессенджеров происходит поверх защищённых протоколов, из-за чего контент переписки практически недоступен для анализа на периметре. DLP-решения вынуждены комбинировать несколько уровней контроля и опираться на контентные и контекстные признаки, однако даже тогда остаются риски и ограничения, связанные с шифрованием и неструктурированными данными [1]. С другой стороны, исследования по DPI и анализу зашифрованного трафика показывают, что по статистическим характеристикам и признакам протоколов можно получать сетевой контекст, но без расшифрования это даёт лишь частичную картину [2]. Следовательно, для веб-мессенджеров актуален гибридный подход, при котором сетевые данные используются для корреляции и верификации, а ключевые события, связанные с попыткой передачи конфиденциальной информации, фиксируются на стороне конечного агента.

Основная часть

В работе предлагается методика обнаружения потенциальных утечек конфиденциальной информации через веб-версии мессенджеров, в частности Telegram Web, VK Web и MAX, ориентированная на корпоративную среду и модель «обнаружение без блокирования». Методика основана на событийной модели: инцидент определяется как попытка передачи конфиденциальных данных наружу независимо от того, завершилась ли доставка сообщения.

Первый уровень — клиентский сенсор в виде браузерного расширения, которое регистрирует пользовательские действия: ввод и вставку текста, попытку отправки сообщения, прикрепление и отправку файлов, копирование фрагментов переписки, а также формирование визуальных артефактов экрана пользователя, для дальнейшей интерпретации в текст и анализа. Такой источник данных позволяет приблизиться к содержательным признакам утечки, которые недоступны на сети из-за шифрования.

Второй уровень — сетевой контур мониторинга, включающий DPI/IDS-инструменты и, при наличии условий, прокси-компонент для обогащения событий контекстом, такие как: временные характеристики, объём передачи, служебные метаданные соединений. Учитывая практическую неприемлемость массового расшифрования трафика, сетевые признаки рассматриваются как механизм корреляции и подтверждения активности, а не как основной канал извлечения контента [2].

Третий уровень — аналитический конвейер, который применяет контентные правила и методы машинного обучения к текстовым и визуальным представлениям данных. Для вложений и изображений используется OCR-этап, после которого признаки передаются в классификатор утечки. Конвейер ориентирован на обработку разнородных типов конфиденциальной информации, таких как персональные данные, документы, содержащие коммерческую тайну и другую информацию, имеющую ценность для предприятия, так же конвейер допускает расширение набора детекторов без изменения клиентской части за счёт унификации формата событий.

Оценка эффективности выполняется на экспериментальном стенде с воспроизводимыми сценариями. Набор данных формируется из открытых источников и синтетических шаблонов, а также дополняется ограниченным объёмом реальных документов организации. Результаты методики сопоставляются с альтернативными вариантами сетевого захвата и анализа трафика, что позволяет количественно и качественно оценить вклад клиентского сенсора и OCR/ML-обработки в условиях повсеместного шифрования. Для формализации области использован опыт работ, посвящённых анализу средств предотвращения утечек конфиденциальных данных [3].

Выводы

Разработана методика обнаружения утечек конфиденциальной информации через приложения для обмена мгновенными сообщениями. Практическая реализация возможна в виде мониторинговой подсистемы, развёртываемой в корпоративном сегменте: браузерное расширение устанавливается на рабочие станции, сетевой контур мониторинга собирает метаданные соединений, а сервер анализа централизованно выполняет корреляцию событий, извлечение текста из визуальных артефактов, классификацию и формирование отчётов по инцидентам. В качестве направления внедрения рассматриваются испытания на типовых сценариях утечки для Telegram Web, VK Web и MAX, а также расширение функциональности управления в последующих версиях решения.

Литература

1. Hauer B. Data Leakage Prevention: A Position to State-of-the-Art Capabilities and Remaining Risk // Proceedings of the 16th International Conference on Enterprise Information Systems (ICEIS-2014). 2014. P. 361–367.
2. Deri L., Sartiano D. Using DPI and Statistical Analysis in Encrypted Network Traffic Monitoring // International Journal for Information Security Research (IJISR). 2020. Vol. 10, Iss. 1. P. 932–943.
3. Губенко Н. Е., Потреба Е. Ю. Анализ методов и средств предотвращения утечек конфиденциальных данных // Проблемы искусственного интеллекта. 2023. С. 55–64.