Отчет статического анализа

На странице статического анализа отображаются результаты анализа статической информации файла, т.е. анализ содержимого файла без его запуска.

В системе tLab уровень угрозы статического анализа вычисляется на основе статических индикаторов угроз, таких как импортирование подозрительных API- функций, наличие скриптов и макросов в документах, аномальная структура секций, шифрованные данные, возможность оперирования на низком уровне, наличие встроенных файлов и т.д.

Отчет статического анализа для разных типов файлов содержит специфическую информацию.

Для исполняемых файлов PE:

- Раскрывающийся список импортируемых модулей и функций;
- Список экспортируемых функций;
- Список извлеченных строк и поиск по частичному совпадению;
- Значок программы;
- Информация о секциях исполняемого файла.
  Для файлов MS Office и PDF: метаданные документа, такие как автор, количество страниц, название, год и т.п.
  Для анализа скриптов:
  - Возможная активность;
  - Обнаруженная активность;

  Для анализа Android приложений:
  - Информация о приложении;
  - Анализ андроида;

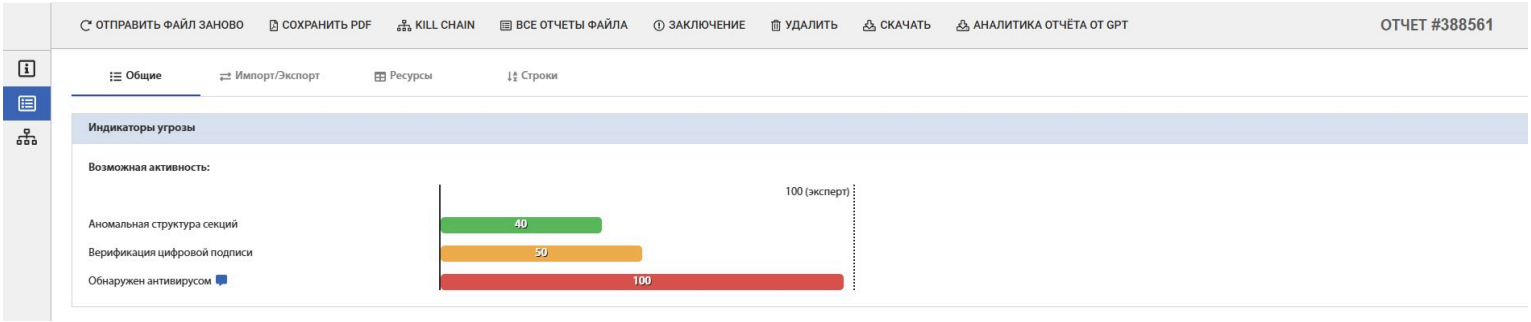

Рис. 14 – Отчет по статическому анализу

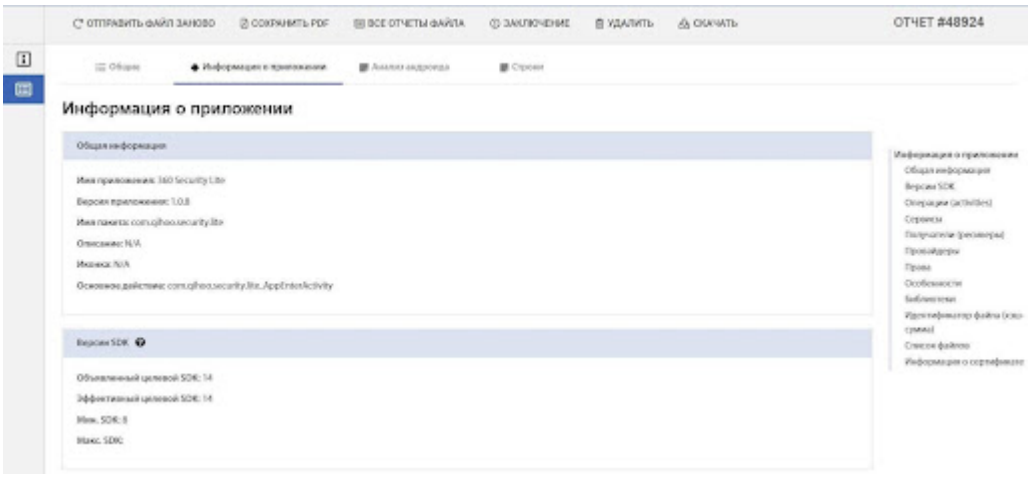

Рис. 14.1 – Отчет по анализу андроид приложения

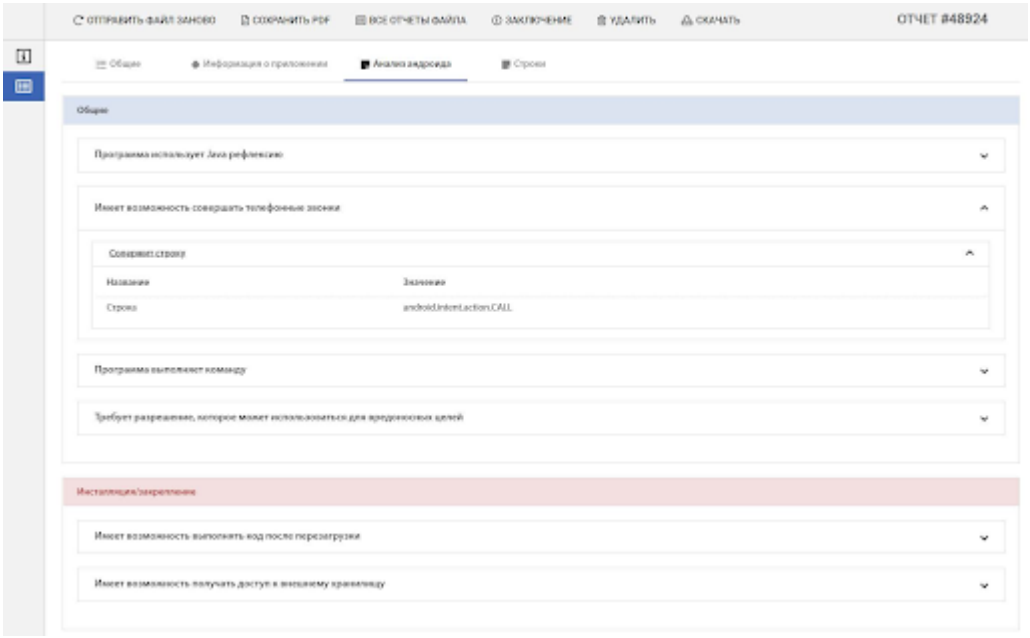

Рис 14.2 – Отчет по анализу андроид приложения

Отредактировать эту страницу