Static Analysis Report

The static analysis page displays the results of analyzing the file's static information, meaning the examination of the file's contents without executing it.

In the tLab system, the threat level of static analysis is calculated based on static threat indicators, such as the import of suspicious API functions, the presence of scripts and macros in documents, anomalous section structures, encrypted data, low-level operations capability, embedded files, and more.

The static analysis report contains specific information depending on the file type.

For PE executable files:

- A collapsible list of imported modules and functions;
- A list of exported functions;
- A list of extracted strings with partial match search functionality;
- Program icon;
- Information about executable file sections.
  For MS Office and PDF files: document metadata such as author, number of pages, title, year, etc.
  For script analysis:
  - Possible activity;
  - Detected activity;

  For Android application analysis:
  - Application information;
  - Android analysis;

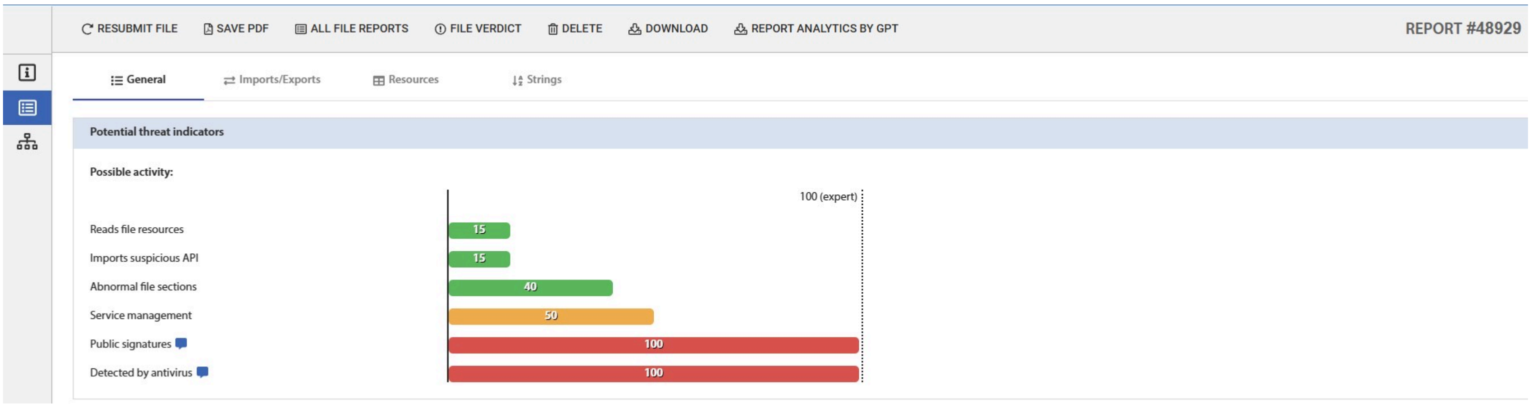
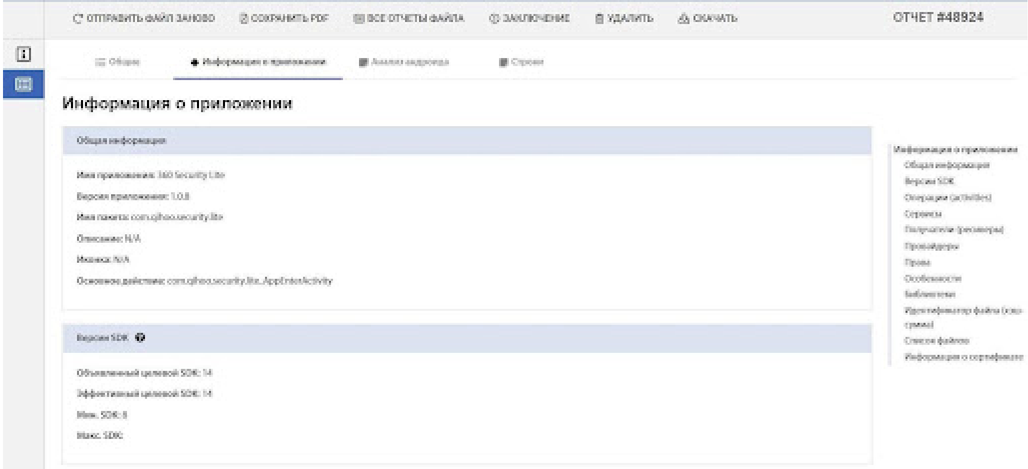


Fig. 14 – Static Analysis Report



Информация о приложении

Общая информация

Имя приложения: 360 Security Lite

Версия приложения: 1.0.8

Имя пакета: com.qihoo.security.lite

Описание: N/A

Иконка: N/A

Основное действие: com.qihoo.security.lite_AppEnterActivity

Версии SDK

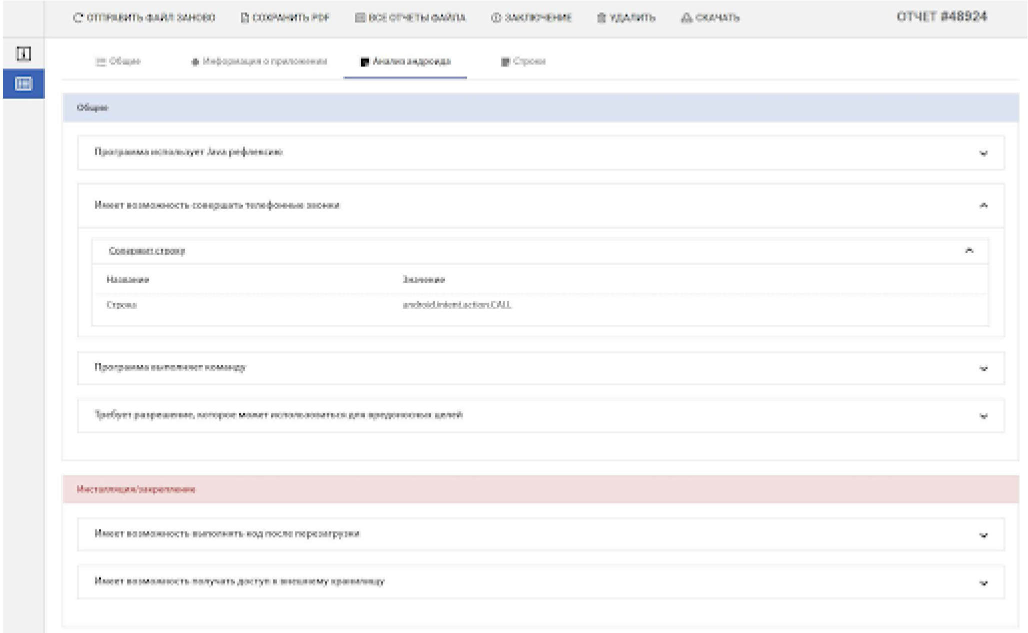
Объявленный целевой SDK: 14

Эффективный целевой SDK: 14

Мин. SDK: 8

Макс. SDK:

Fig. 14.1 – Android Application Analysis Report



Общее

Программа использует Java рефлексию

Имеет возможность совершать телефонные звонки

Содержит строку

Название	Значение
Строка	android.intent.action.CALL

Программа выполняет команду

Требует разрешение, которое может использоваться для вредоносных целей

Инсталляция/закрепление

Имеет возможность выполнять код после перезагрузки

Имеет возможность получать доступ к внешнему хранилищу

Fig. 14.2 – Android Application Analysis Report

Edit this page