



DeepSlicer

DeepSlicer - статический анализатор. Читает текст скрипта, определяет язык, на котором он написан и выдает информацию о его подозрительном функционале без непосредственного запуска. Например, запись в реестр или скачивание файлов.

На рисунке 14.3.1 изображена возможная активность - функции, которые присутствуют в коде, но возможно не запускаются.

На рисунке 14.3.2 изображена обнаруженная активность - функции, которые вызываются в коде.



ВНИМАНИЕ

Стоит обратить внимание на потенциально вредоносную активность

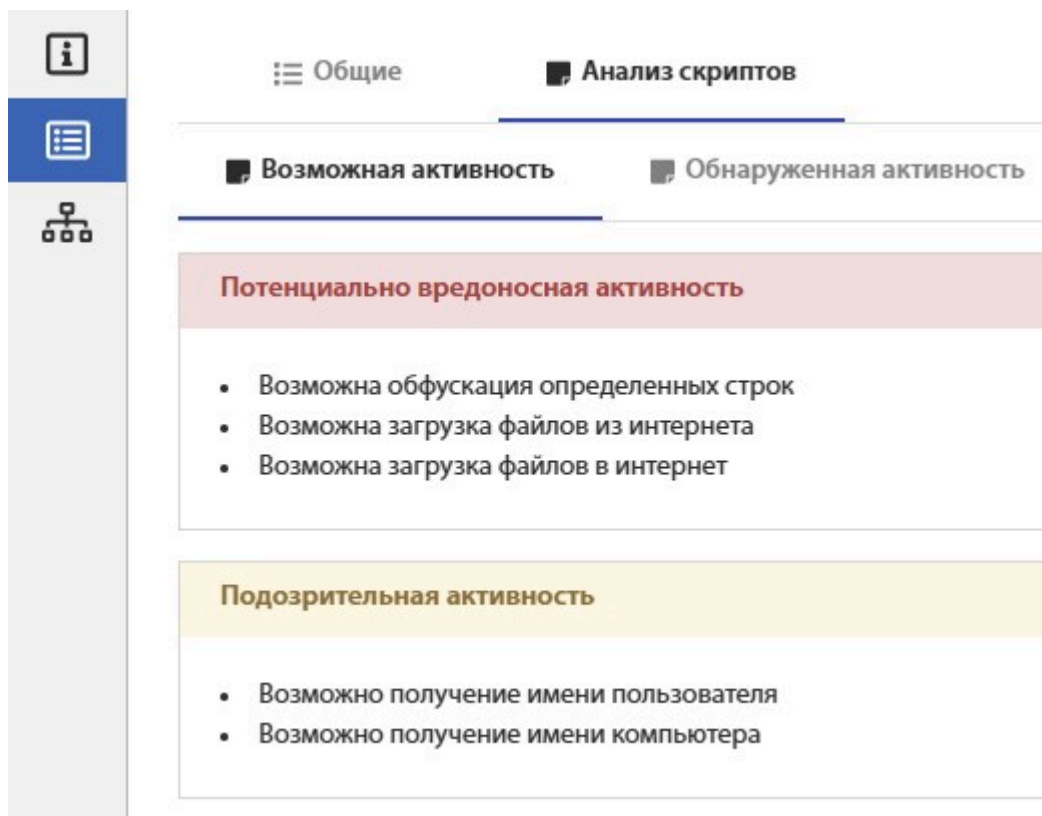


Рис. 14.3.1 - страница DeepSlicer: возможная активность

Общие

Анализ скриптов

Возможная активность

Обнаруженная активность

Потенциально вредоносная активность

Внедрение VBA-кода в новый документ Word (через управление другим экземпляром Word)

1


Подозрительная активность

Попытка работы с HEX

1

Попытка записи в реестр

1

Address	Name	Value	Type	Extra
 HKCU\Software\Microsoft\Office\application.version\Word\Security	AccessVBOM	1	REG_DWORD	No information

Создание нового документа через удалённое управление другим экземпляром Word

1

Общая активность

Попытка создания OLE объектов

1

Рис. 14.3.2 - страница DeepSlicer: обнаруженная активность

Общие

Легитимная активность

События

Макросы содержат не только подпрограммы

1

Рис. 14.3.3 - страница DeepSlicer: легитимная активность

 [Отредактировать эту страницу](#)