

# 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

Стоить обратить внимание на потенциально вредоносную активность

The screenshot shows the DeepSlicer user interface. On the left is a vertical sidebar with three icons: a blue square with an 'i' (Information), a blue document icon (Report), and a blue tree icon (Analysis). The main area has a light yellow header bar with the title 'Анализ скриптов' (Script Analysis) in bold black text. Below the header, there are two tabs: 'Возможная активность' (Potential Activity) and 'Обнаруженная активность' (Detected Activity), with 'Возможная активность' currently selected. A red box highlights the title 'Потенциально вредоносная активность' (Potentially Malicious Activity). Below it is a list of three items:

- Возможна обfuscация определенных строк
- Возможна загрузка файлов из интернета
- Возможна загрузка файлов в интернет

Below this section is another red box highlighting the title 'Подозрительная активность' (Suspicious Activity). Below it is a list of two items:

- Возможно получение имени пользователя
- Возможно получение имени компьютера

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