DeepSlicer

DeepSlicer is a static analyzer. It reads the script text, determines the language in which it is written, and provides information about its suspicious functionality without direct execution, such as registry modifications or file download.

In Fig. 14.3.1, potential activity is shown – functions that are present in the code but may not be executed.

In Fig. 14.3.2, detected activity is shown – functions that are explicitly called in the code.
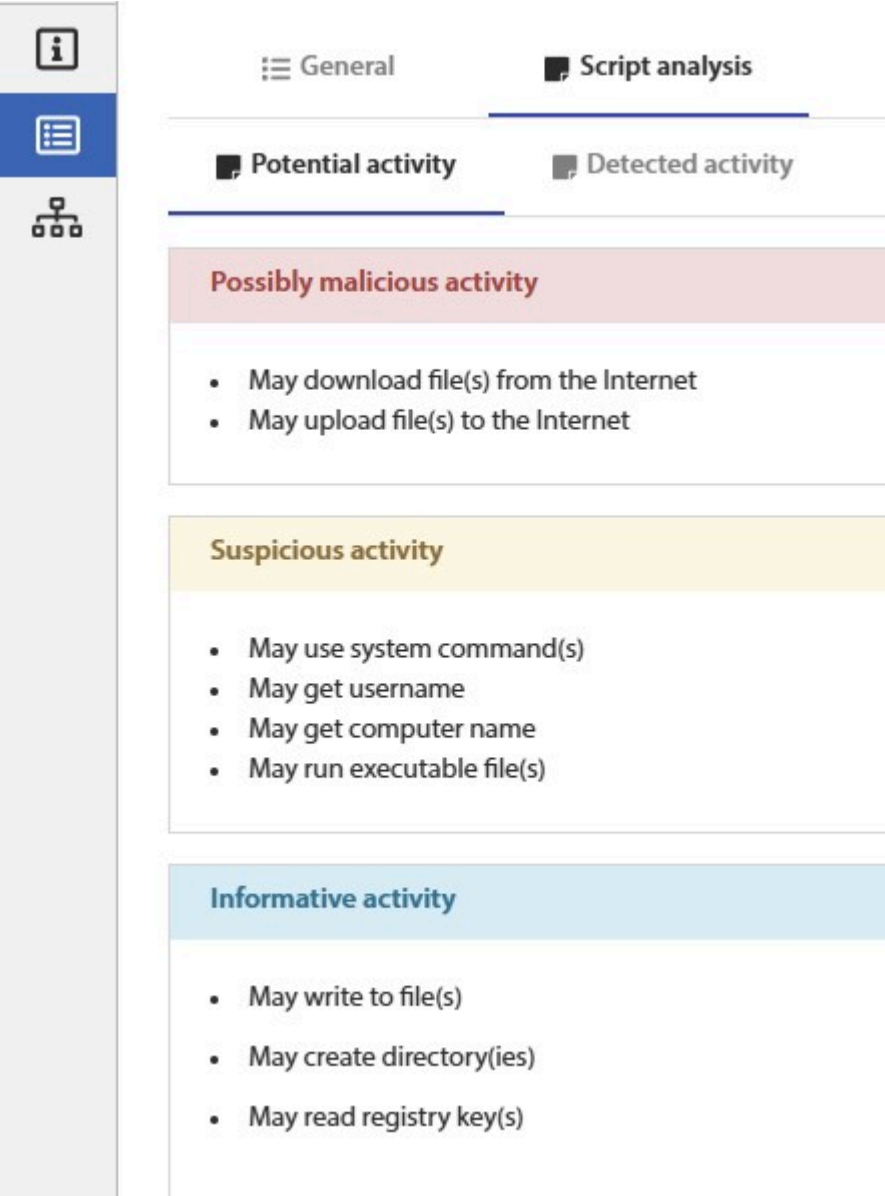
> ⚠️ **WARNING**
>
> Pay attention to potentially malicious activity.
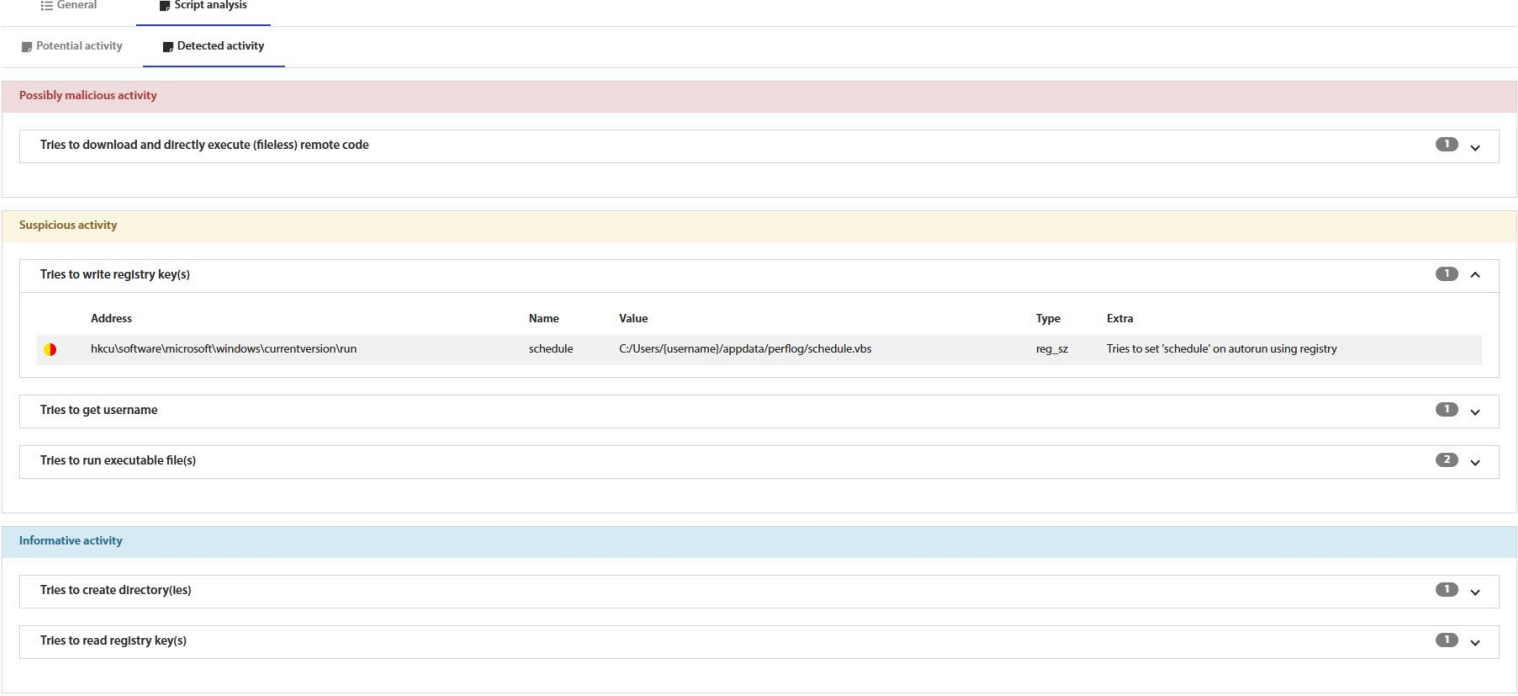

Fig. 14.3.1 – DeepSlicer Page: Potential Activity

Possibly malicious activity

Tries to download and directly execute (fileless) remote code	① ⌄

Suspicious activity

Tries to write registry key(s)   ① ⌃

	Address	Name	Value	Type	Extra
🔴	hkcu\software\microsoft\windows\currentversion\run	schedule	C:/Users/[username]/appdata/perflog/schedule.vbs	reg_sz	Tries to set 'schedule' on autorun using registry

Tries to get username	① ⌄

Tries to run executable file(s)	② ⌄

Informative activity

Tries to create directory(ies)	① ⌄

Tries to read registry key(s)	① ⌄

Fig. 14.3.2 – DeepSlicer Page: Detected Activity

События

Макросы содержат не только подпрограммы	① ⌄

Fig. 14.3.3 – DeepSlicer Page: Legitimate Activity

✏ Edit this page