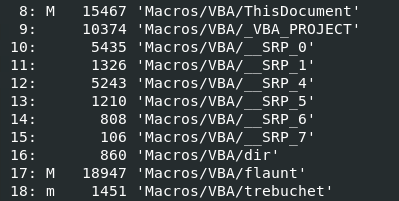
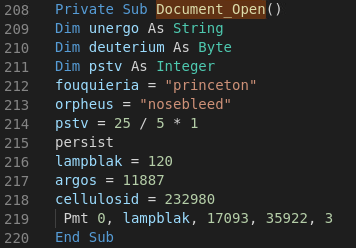
Lab 02

Please provide detailed responses using text as well as when appropriate screenshots. Answers that one sentence, one screenshot, minimal effort, etc., will be graded accordingly.

**Part 1**

Respond to **each** of the below items.

* What stream does the malware begin at? Where does it lead you to next? How can you tell? Include screenshot.

Inside of stream 8, there is a function called Document\_Open() which calls the functions persist, and Pmt.

Persist is defined above in the same stream – it’s pretty long so I wont include the whole thing in the screencap. Pmt seems irrelevant for our purposes, it’s a VBA function for annuity payment calculations. And it appears in several places throughout the stream.

* What Windows API functions are used? Hint: look at the aliases. List each and provide a brief description of what each does. You will need to look each up through MSDN. Put in your own words.
* Which API functions are used in the malware, and what parameters are provided to each? As best as you can determine, provide the functions in the order in which they are used. What do you think each is trying to do? Sometimes malware may also use a function in an unorthodox way.
* Is the word doc hiding something in it besides the streams? What clues may lead you to conclude this? What is it?
* Is there shellcode in there that you can capture? Open it up in IDA or other tool at the entry point.

**Deliverable**

* A Word document or PDF with requested answers to the previous tasks.
* No zip files – please upload multiple files if ever needed.