Delivery Mechanisms:

**JavaScript attachments**

# Malware Activity

**Lab Description:** This lab will be presented with one file from a word document with an attached JavaScript file.

**Lab Environment:** Use of variety of tools is needed for this lab. It is recommended to do this lab in a virtualized environment. The file being provided is malware.

**Lab Files that are Needed:**

Malware.zip which holds maintools.js – the zip file containing this sample is password protected with a password of: infected

### Lab Exercise 1

*Learning Outcomes 1, 2, & 3*

Using the method, you prefer to modify the file. Follow the questions and provide screen shots for each.

* Identify the statement that is running the malware?
* Modify the code to print the deobfuscated file.
* Explain why this can’t be done with a print statement?

### Lab Exercise 2

*Learning Outcomes 1 & 2*

Using a sandbox look up the following question.

* Is this file identified on the sandbox using md5sum or sha256?

### Lab Exercise 3

*Learning Outcomes 1, 2, & 3*

* Export the deobfuscated file to a new JavaScript file. Show the command line used to execute this.
* What are the different address the malware dropper is attempting to get to?

# What to submit

Submissions should be neatly organized. Each question should include at least one screenshot and a brief explanation if possible.