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

### **Lab Exercise 1**

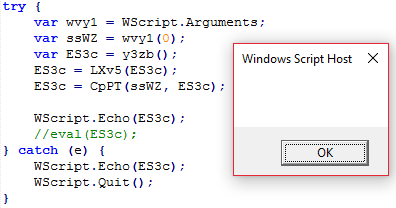
*Learning Outcomes 1, 2, & 3*

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?

Eval runs statement to deobfuscated 

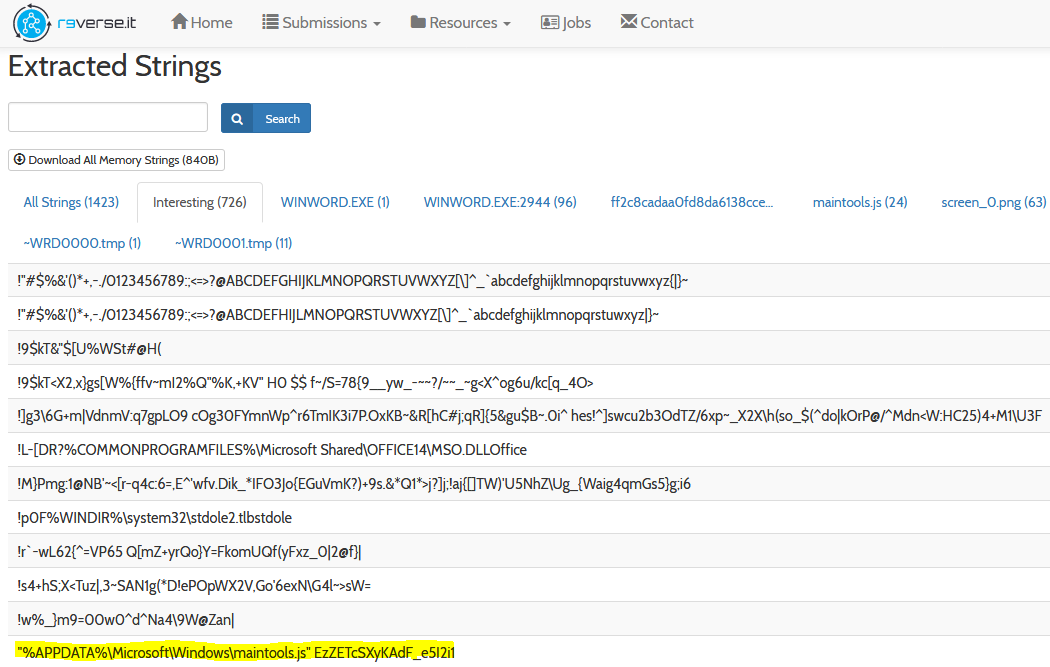
* Modify the code to print the deobfuscated file.



This code will print the file but when run it needs the correct command line argument to deobfuscate it correctly.

* Explain why this can’t be done with a print statement?

The reason is the file needs a key to be entered with it so it will deobfuscate correctly. This can be found by looking the md5sum or sha256 up online.



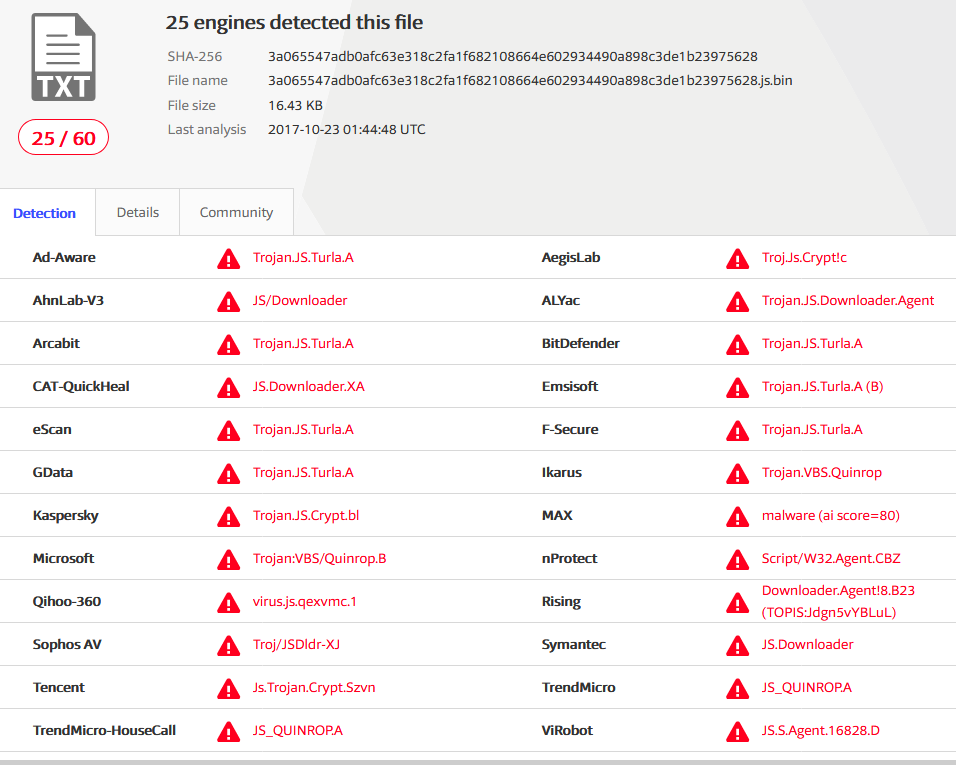
### **Lab Exercise 2**

*Learning Outcomes 1 & 2*

Using a sandbox look up the following question.

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

Yes, it is identified by virus total.



### **Lab Exercise 3**

* Export the deobfuscated file to a new JavaScript file. Show the command line used to execute this.

Example of running the file

* What are the different address the malware dropper is attempting to get to?

Websites it reaches out too

# What to submit

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