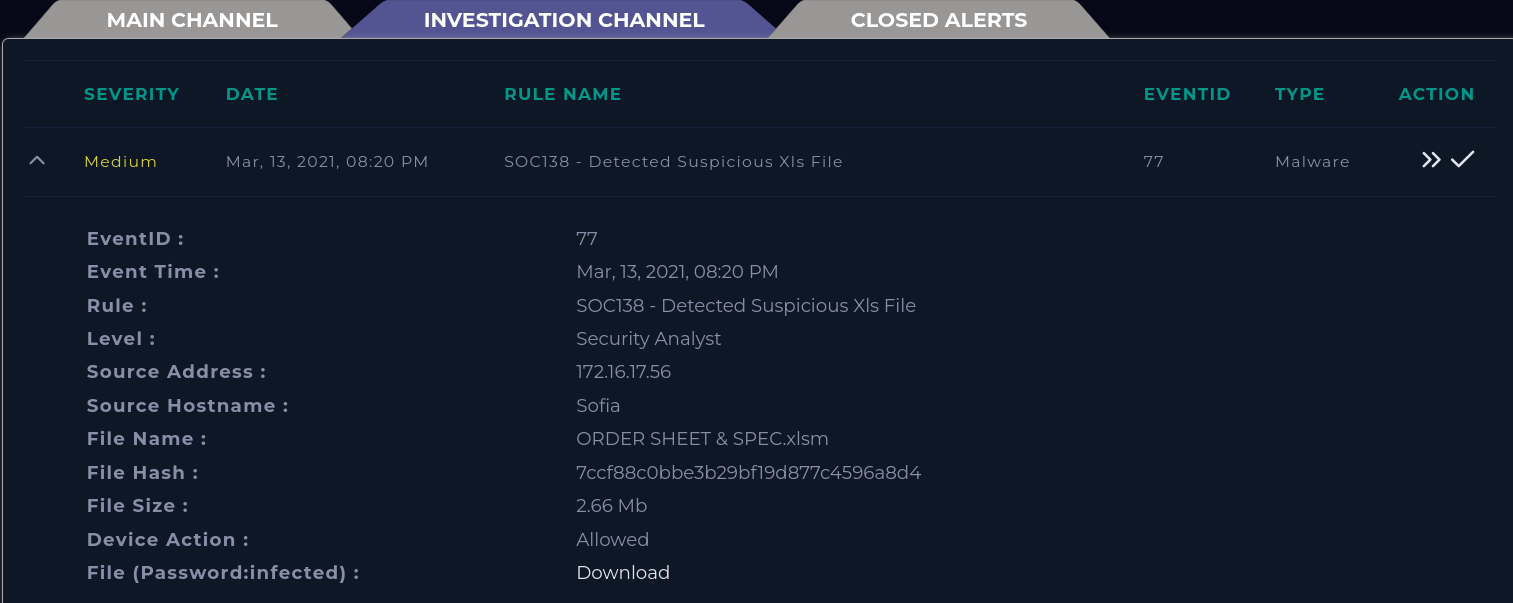
I am going to be creating a case on LetsDefend’s “SOC138 - Detected Suspicious Xls File” alert.



First, Let’s the information from the alert itself.

When did the alert occur?

Mar, 13, 2021, 08:20 PM

What’s the source address and hostname?

172.16.17.56 Sofia

What’s the file name?

ORDER SHEET & SPEC.xlsm

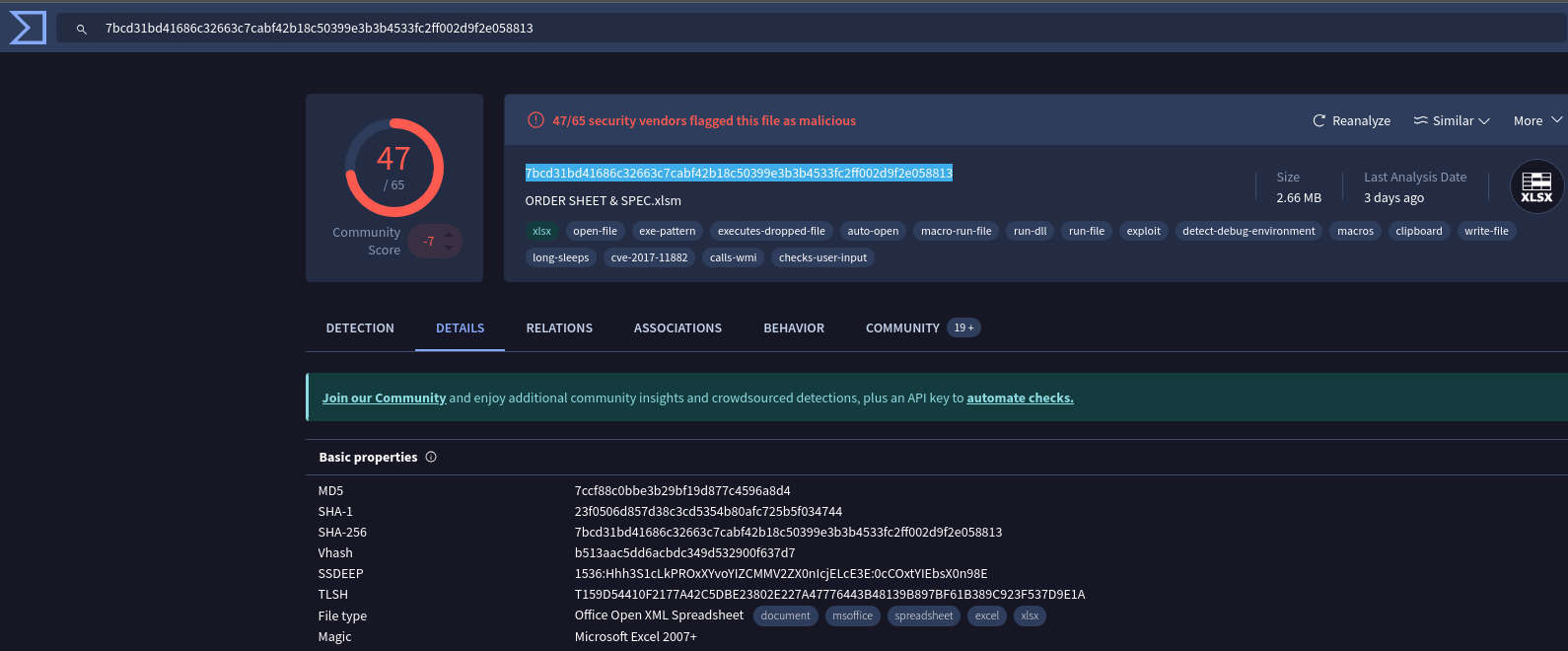
What’s the file hash?

7ccf88c0bbe3b29bf19d877c4596a8d4

Why did the alert occur?

Detection of a potentially malicious Microsoft Excel (Xls) file.

Let’s start the investigation by searching the file hash on virus total. Virus total shows that the Excel attachment is likely malicious.



Next let's perform some dynamic testing using an [Any.run](https://any.run/) virtual machine. Creating a virtual machine using the malicious file download URL. Starting the virtual machine