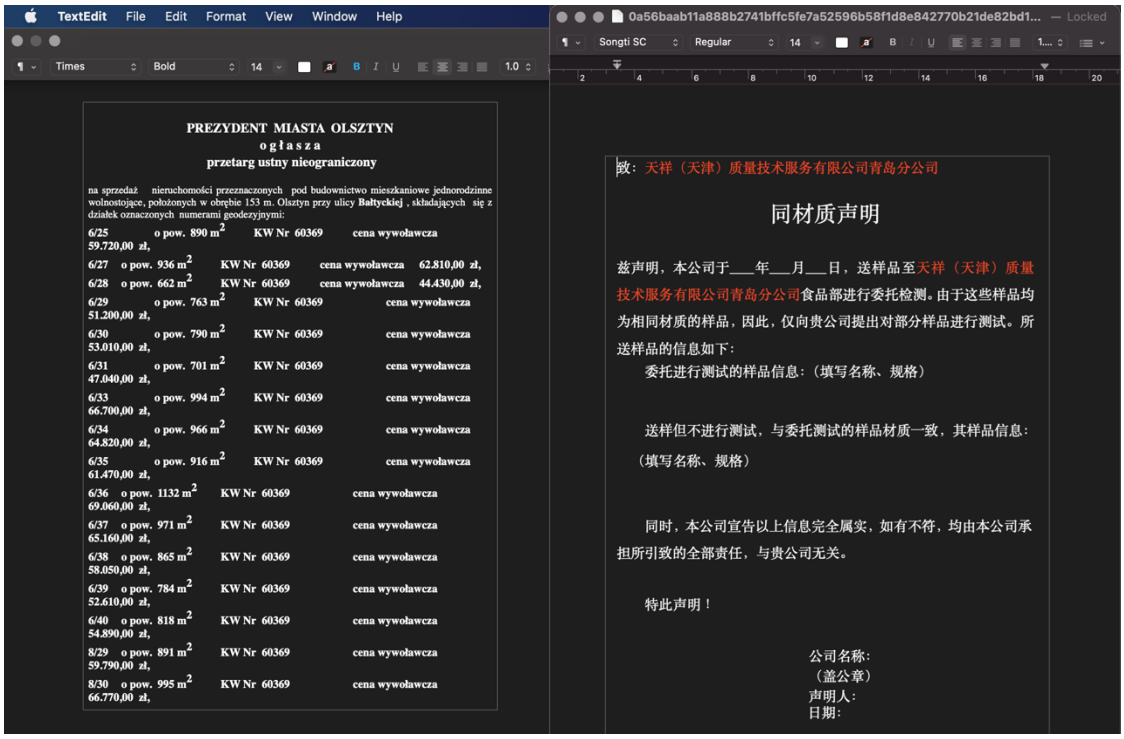
Melissa – Macro worm analysis report

About the Malware type

The Melissa virus was a mass-mailing macro virus. It targeted Microsoft Word and Outlook-based systems and created considerable network traffic. The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first fifty people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.
Source – [Wikipedia]

File type analysis

Analyzing the contents of the document file



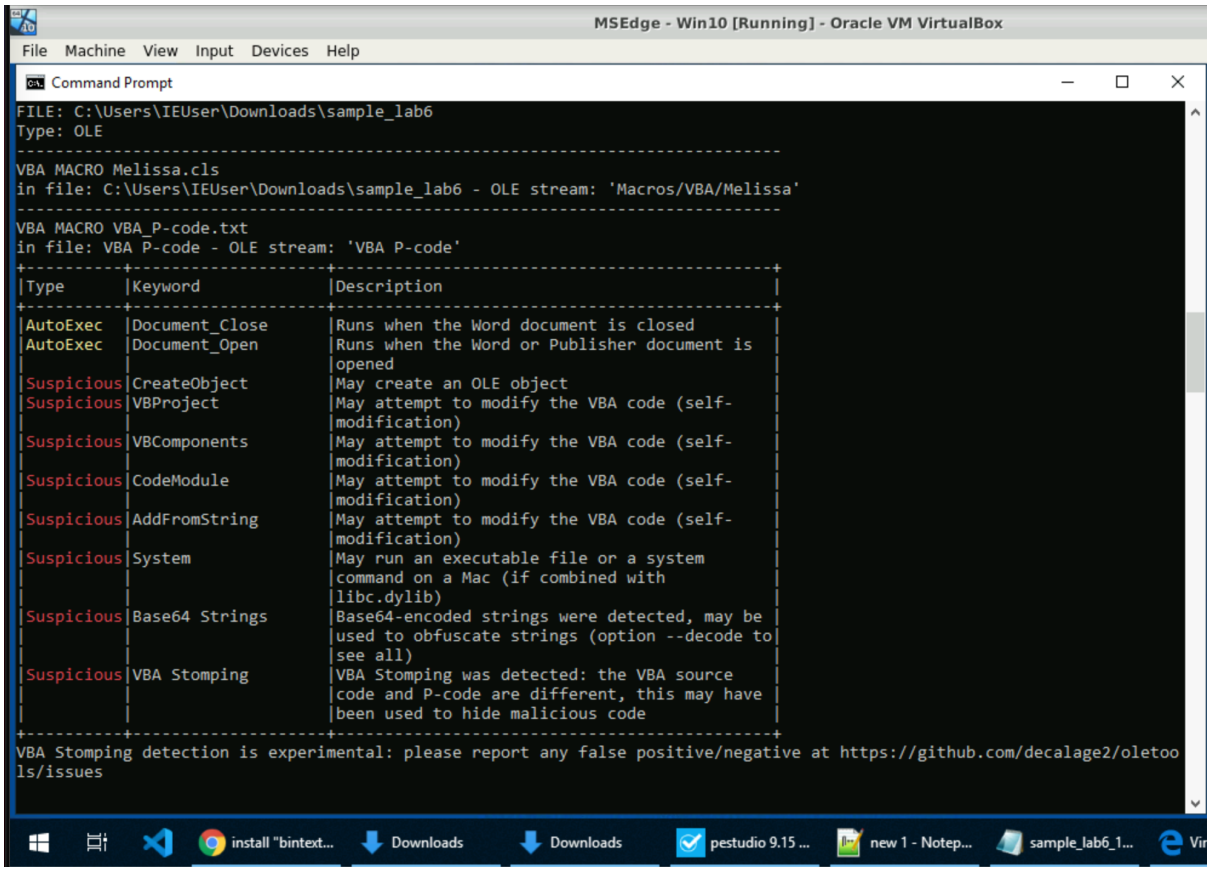
Analyzing the file header

(Wikipedia)

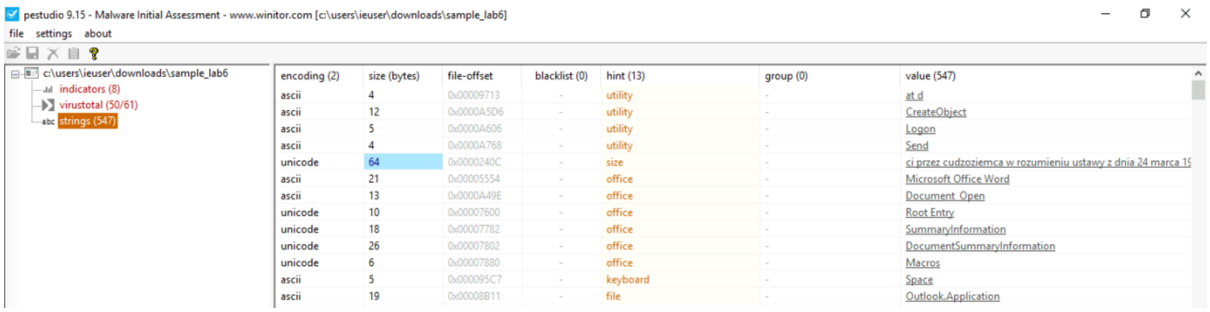
D0 CF 11 E0 A1 B1 1A E1	ÐÏ ∞ à ± ᵃᵉ á	0	doc xls ppt msg	Compound File Binary Format, a container format used for document by older versions of Microsoft Office.[27] It is however an open format used by other programs as well.

Type of file: **Microsoft Word 97-2003 Document**

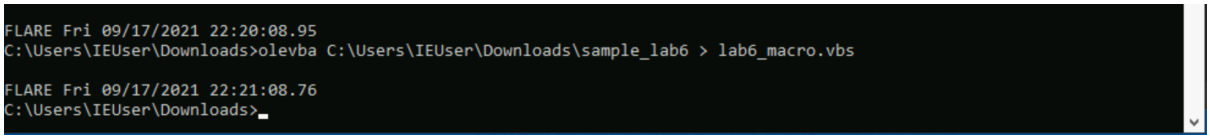
Static analysis using OLE VBA tool



Strings from PEStudio

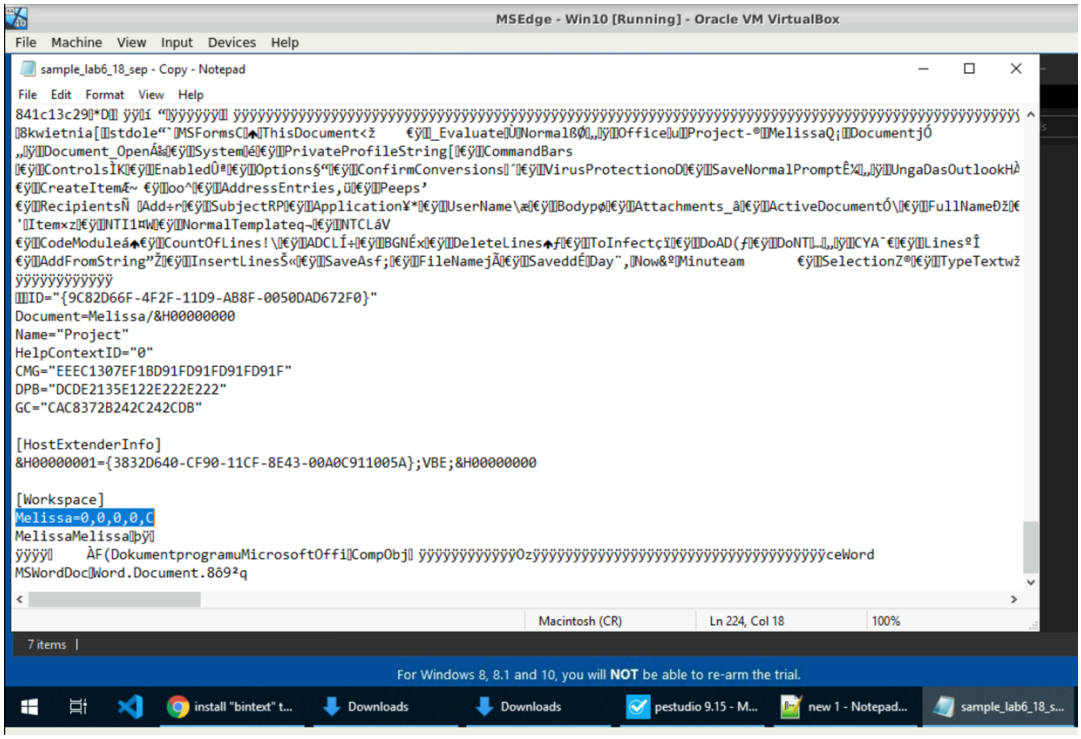


Extracting the macro inside the word file

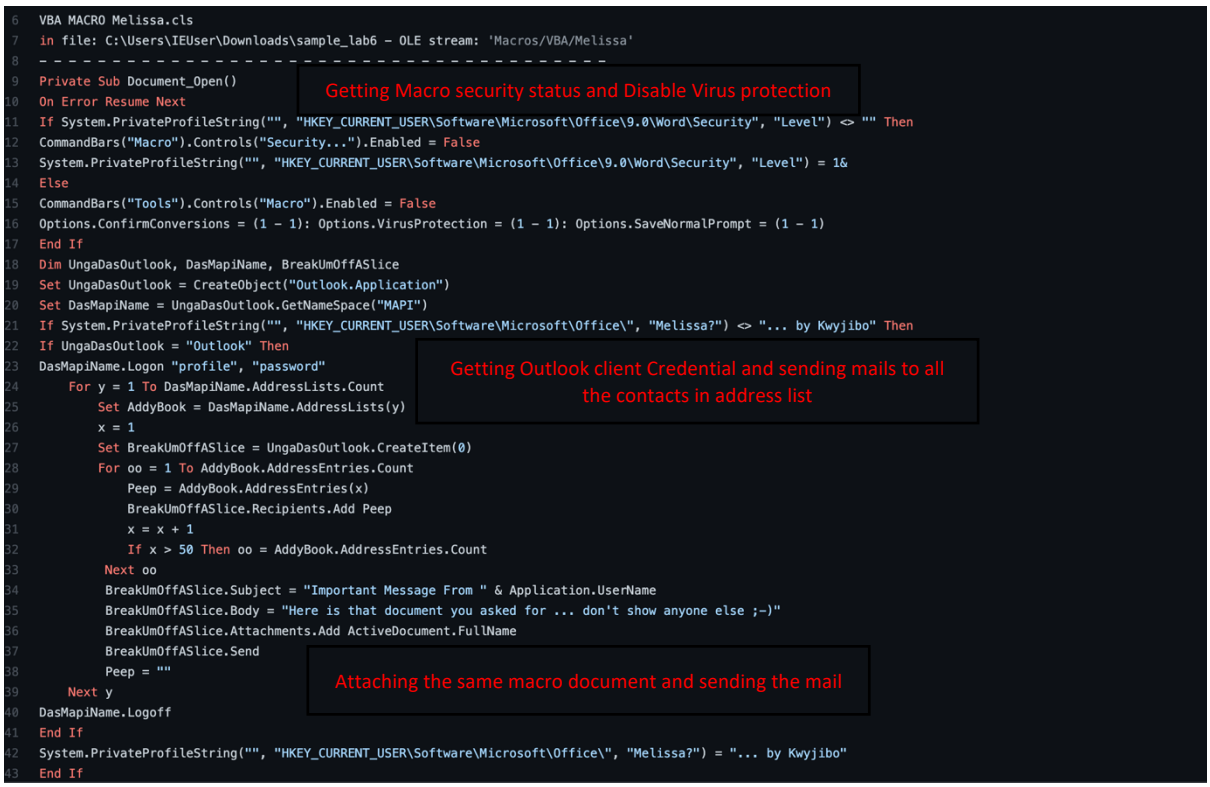


The contents of Macro help to identify the functionalities of the malware and it's interaction with victim system as shown in below section

File content after removing space



What the file will do?



Similar malwares

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
c080b19619315c395365c270c698c9afd6d082dc43e33e2ed31baf6df27df2e0
08531e5b37745d037f5c63829f04c425f9e2631bed6a5aea5c447e586d2b938d

Yara rule

```
rule melissa

{

meta:

created = "18/09/2021 11:15:00 AM IST"
modified = "18/09/2021 11:55:00 AM IST"
author= "vijayabharathi"
description = "To find Melissa Macro worm using strings"

strings:

$str1 = "Kwyjibo"
$str2 = "Here is that document you asked for ... don't show anyone else ;-)"
$str3 = "Melissa/&H00000000"
$str4 = "Important Message From"
$str5 = "Game's over.  I'm outta here"
$str6 = "Outlook.Application"
$str7 = "Macro Virus"

condition:

all of them

}
```

Yara rule – output