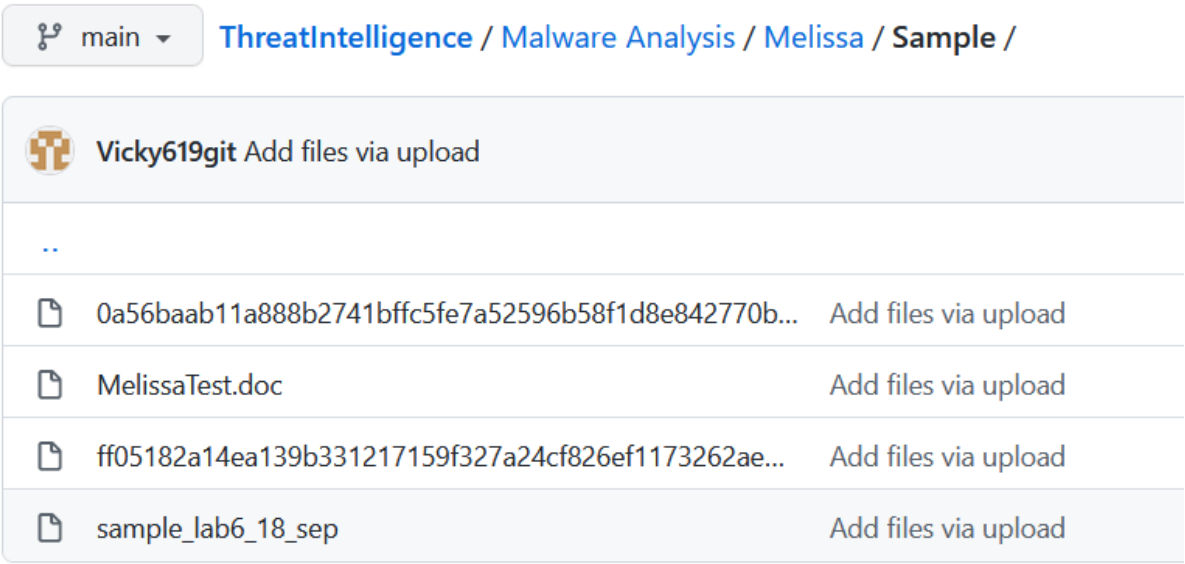
THREAT INTELLIGENCE LAB ASSIGNMENT

ASSIGNMENT:

- Get the sample from same course GIT repo filename:sample_lab6_18_sep
- Create report with following details
    1. <type of file>
    2. <Static analysis>
    3. <what file do>
    4. <Threat Intel (collect similar file info from wild)>
    5. <Yara rule>

SAMPLE:

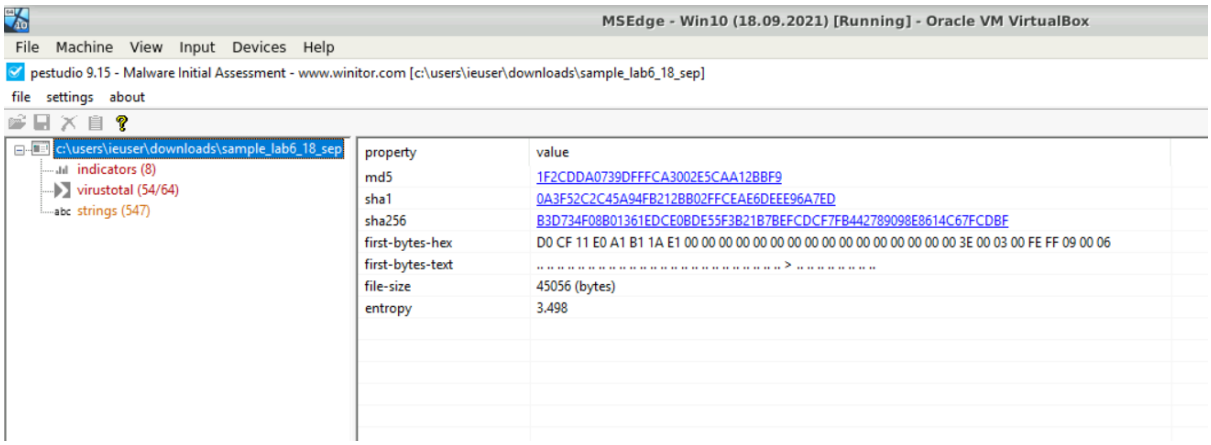
https://github.com/Vicky619git/ThreatIntelligence/tree/main/Malware%20Analysis/Melissa/Sample



STATIC ANALYSIS USING PESTUDIO:

PeStudio is a free tool that allows you to do the static investigation of any Windows executable binary. A file being analysed with PeStudio is never launched; therefore, you can evaluate unknown executable and even malware with no risk.

Sample: sample_lab6_18_sep

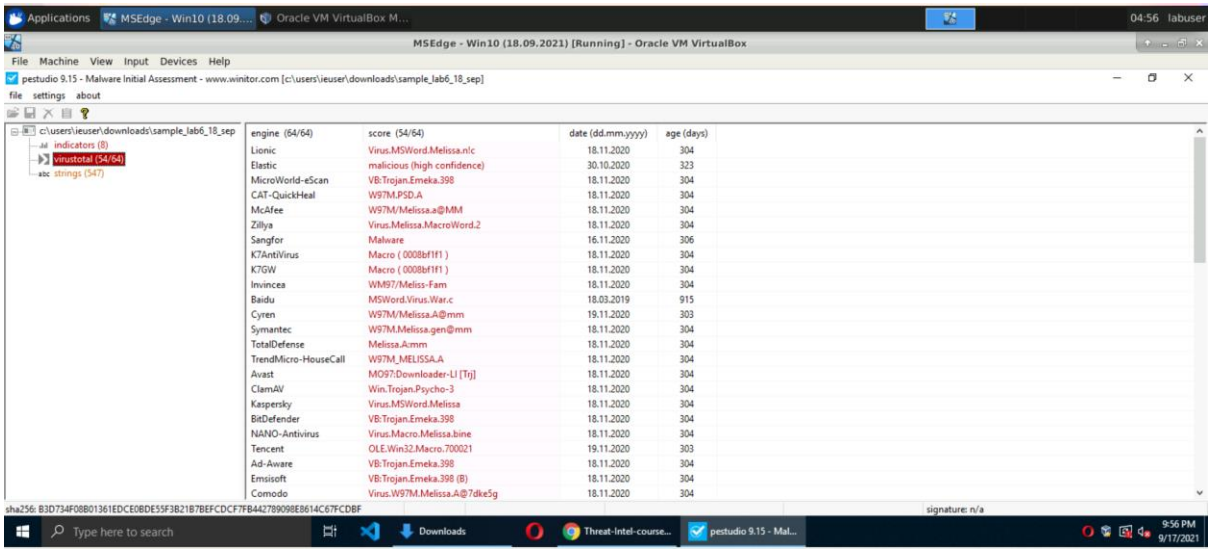


First-bytes: D0 CF

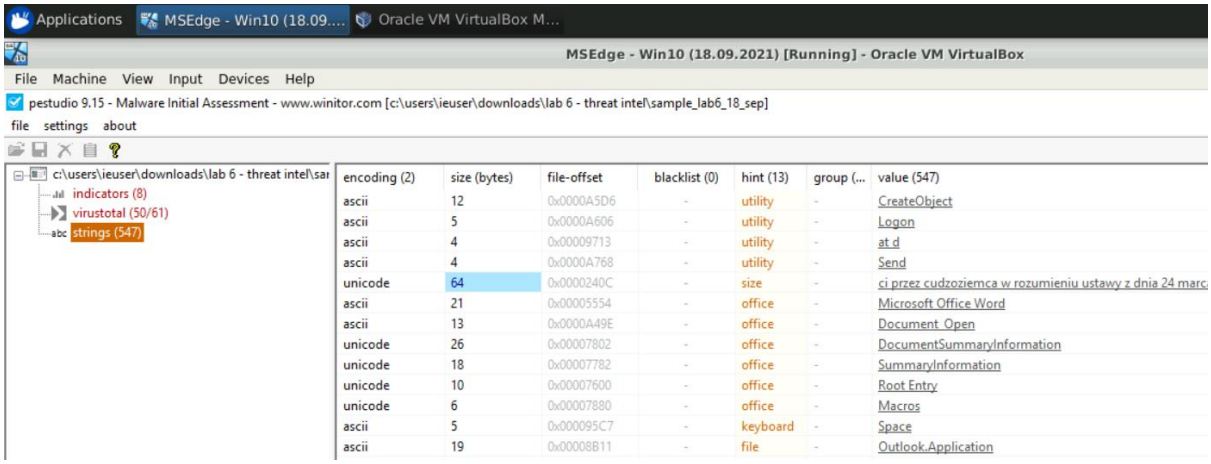
File type: (doc, xls, ppt, msg) Compound File Binary Format, a container format used for document by older versions of Microsoft Office. It is however an open format used by other programs as well. MS Word Document. (https://en.wikipedia.org/wiki/List_of_file_signatures)

SHA-256: b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbfs

File size: 44.00 KB (45056 bytes)

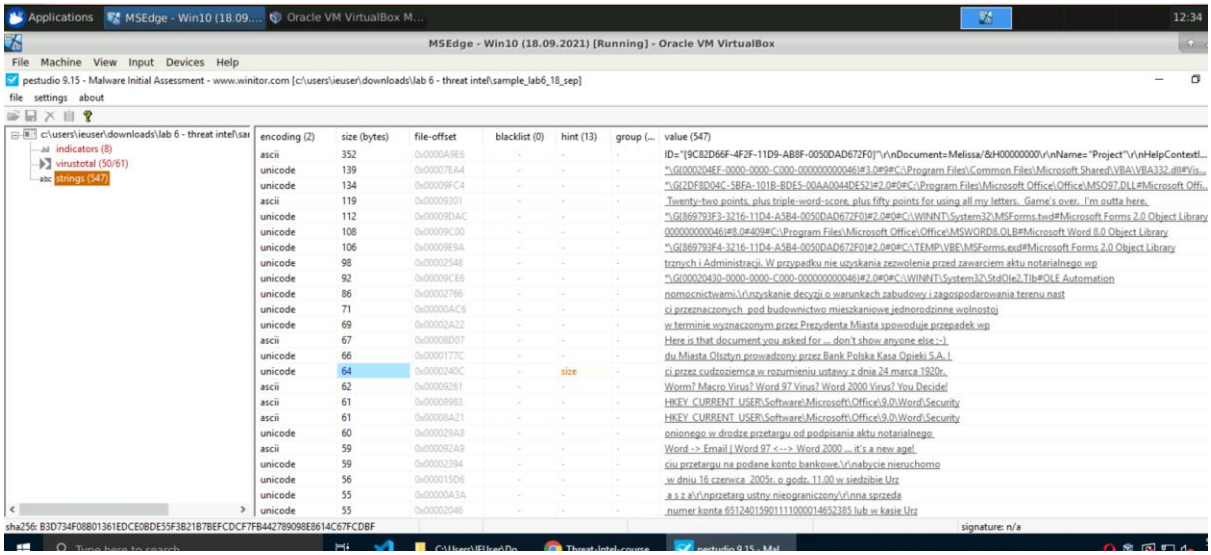


54 out of 64 confirm this sample to be malicious and Majority of AV engines specify the malware to be Melissa (W97M/Melissa).



Here we can see that some of the strings are Microsoft Office Word, Macros, Outlook Application and Root entry etc.

Therefore, this malware sample uses macros and outlook application to spread. Create Object, Document Open, Send string values states that the malware tries to open the document file and modify and send using outlook.



In the above screenshot, there are some strings which were displayed during the execution of the malware. Some of them are like

- Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.
- Here is that document you asked for ... don't show anyone else ;-)
- Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
- Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
- WORD/Melissa written by Kwyjibo
- Important Message From

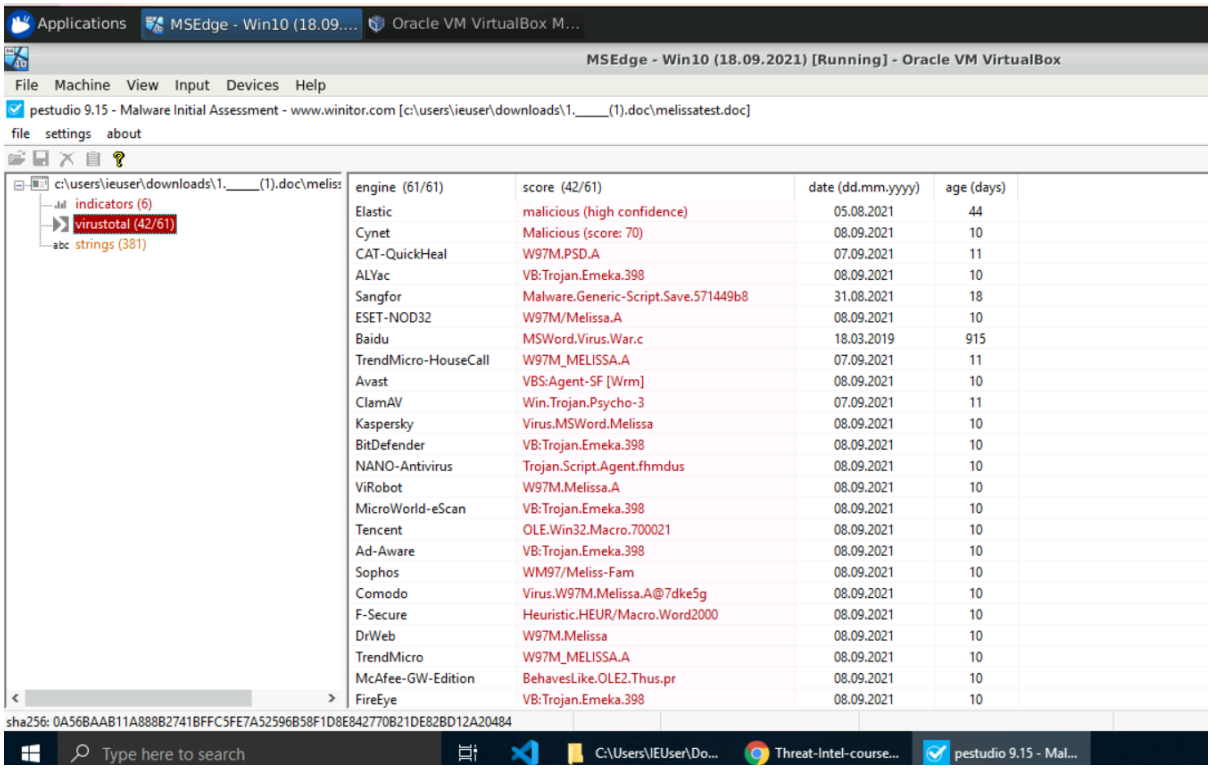
Similar analysis is done on another sample:

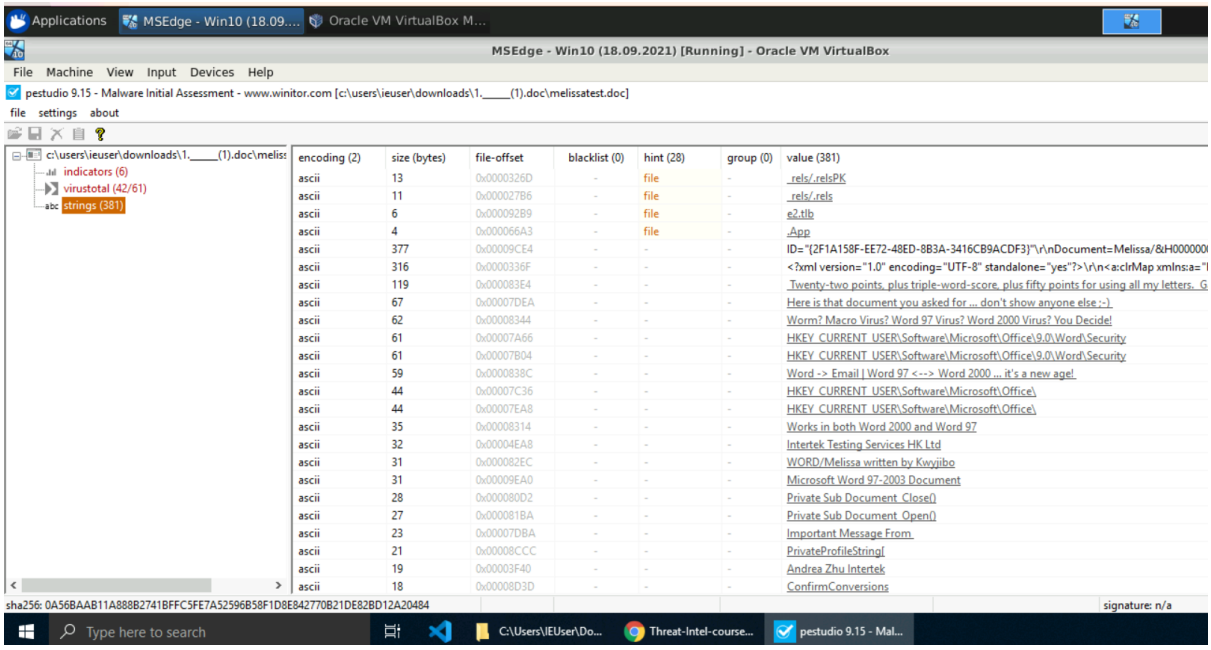
From the list of MD5 hashes provided:

51a319db15b885161702caf96ac6f0de; 02cd26ed2813d996d4d9d1277636dd91; 3fa51b2984d79bc69a280870e4387cf0; 2b1f13e2948b9b473ad4c3eb6a852ea7; 264ffd5eaed5cf99848fbd310628a162; c6118068b71c72b7f2b4428d27132400; 8ec1528c7f12264808eaf2ac1eafeb6; e90ed77286e7d685ac3809f366f19d75 and 045cb8ecf9a4b99d30f66911acb250b6

I was able to download one sample file from Anyrun website

MelissaTest.doc (MD5 - 02cd26ed2813d996d4d9d1277636dd91)





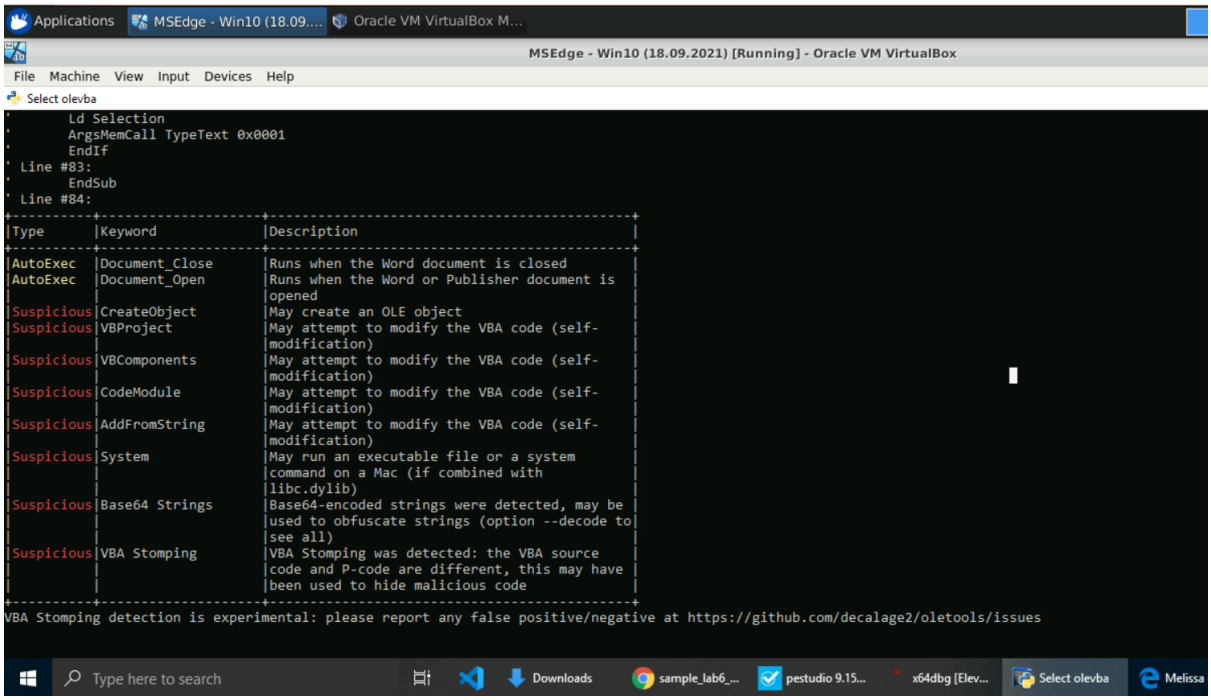
The string patterns are mostly similar in both the samples taken

OLEVBA:

OLEVBA is a tool to extract VBA Macro source code from MS Office documents. Supported formats are:

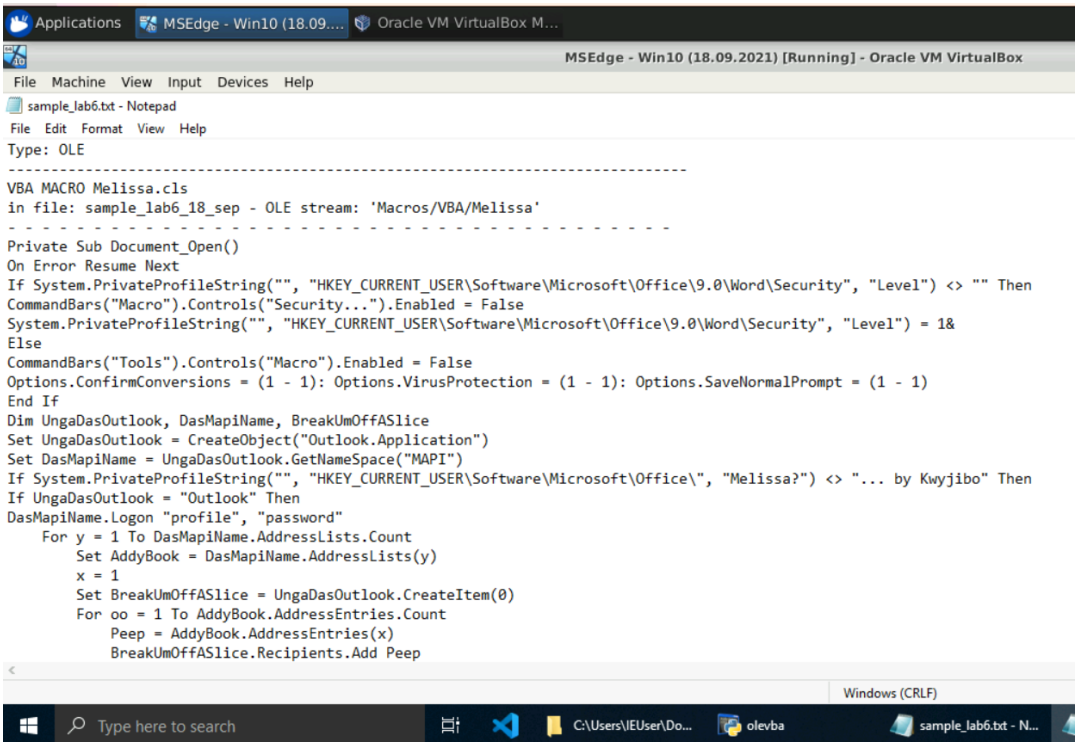
- Word 97-2003 (.doc, .dot), Word 2007+ (.docm, .dotm)
- Excel 97-2003 (.xls), Excel 2007+ (.xlsm, .xlsb)
- PowerPoint 2007+ (.pptm, .ppsm)

Since the samples are macro embedded, we are going to use OLEVBA to analyse the samples.



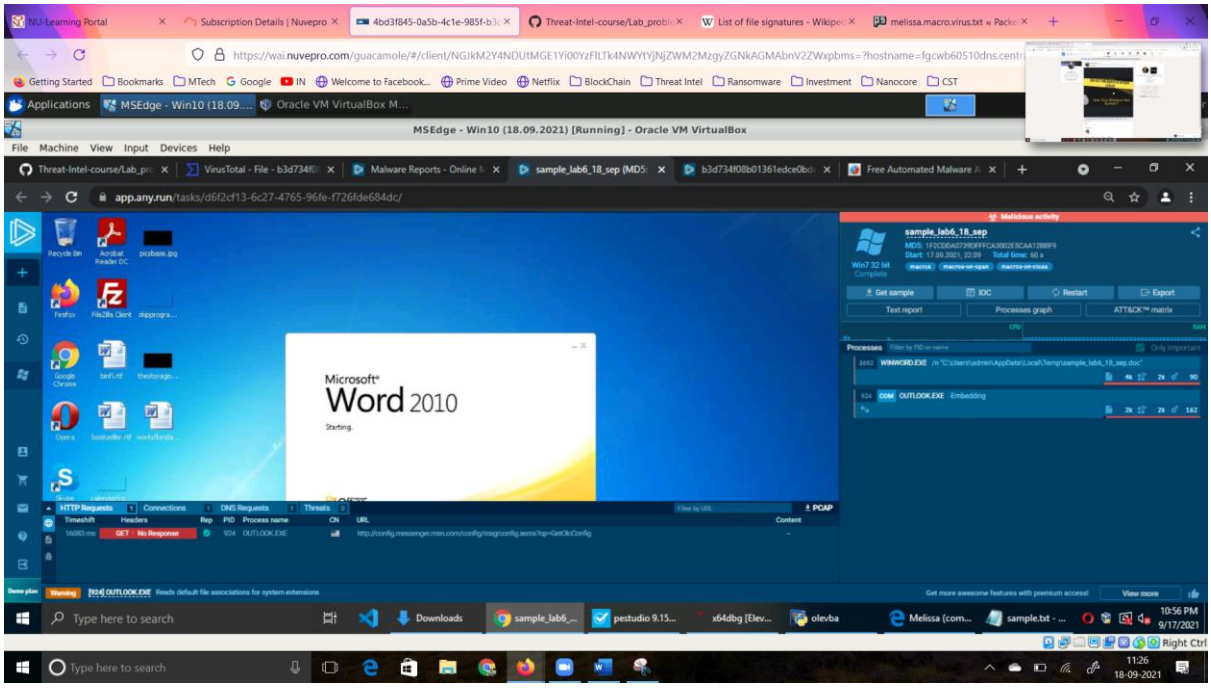
The OLEVBA Output from both the samples are attached in the Git repo

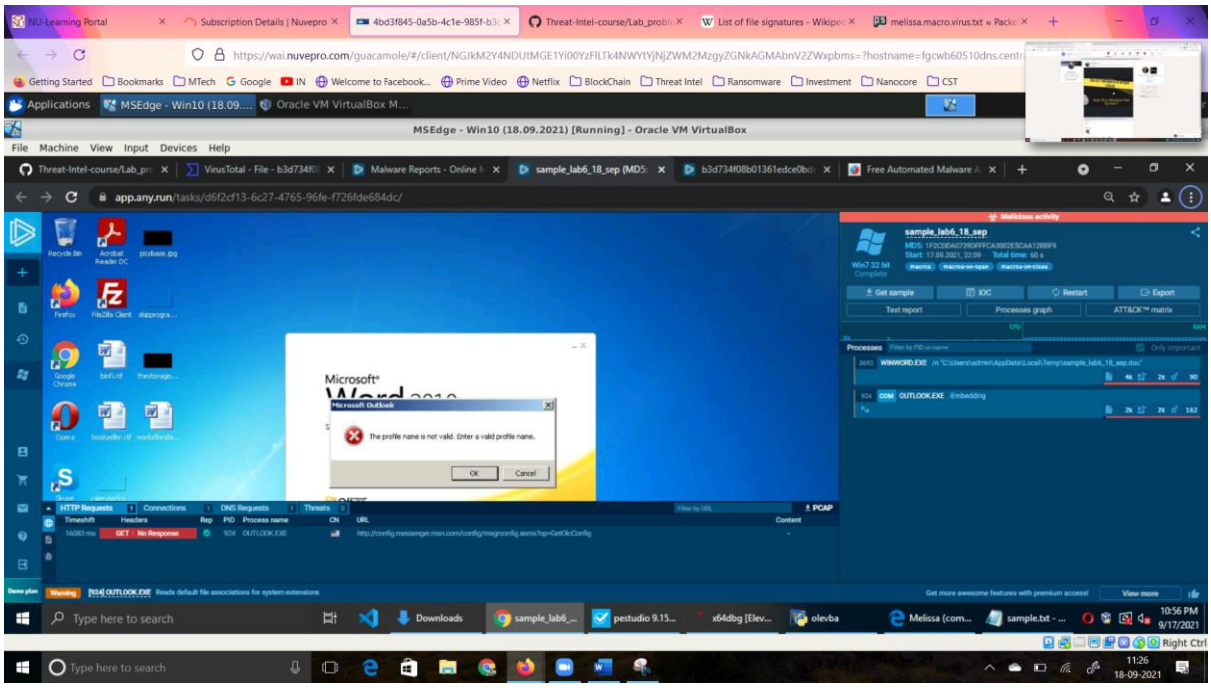
https://github.com/Vicky619git/ThreatIntelligence/blob/main/Malware%20Analysis/Melissa/OLEVBA%20Output/sample_lab6.txt

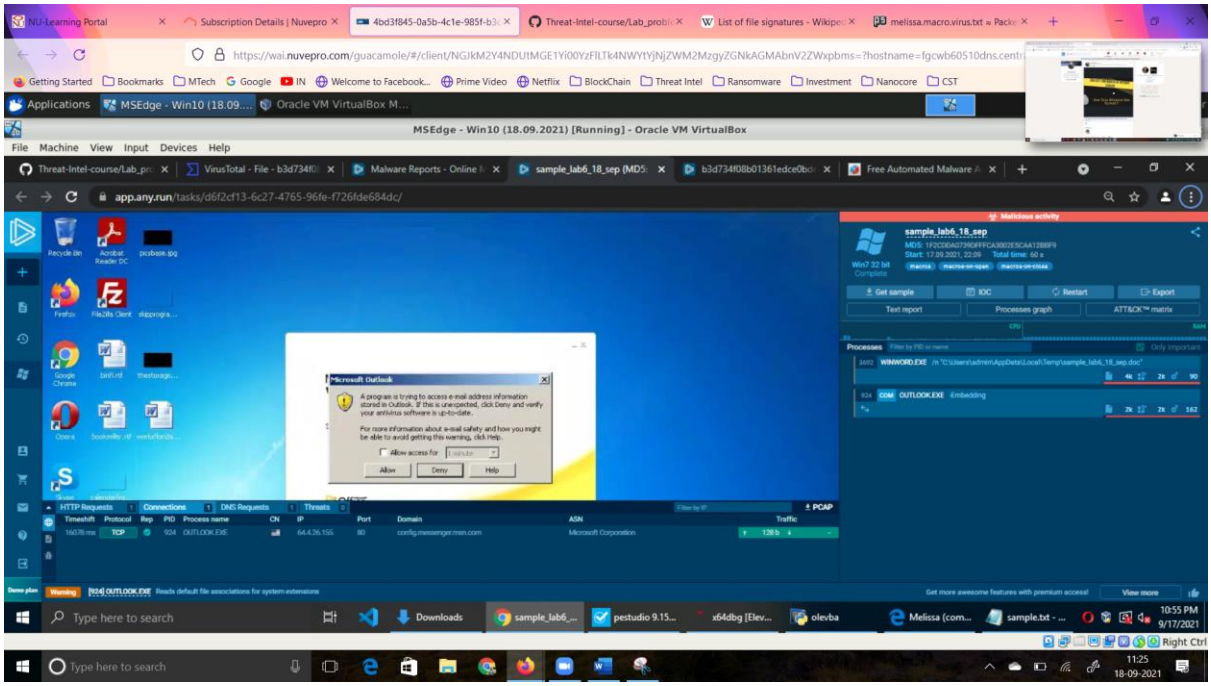


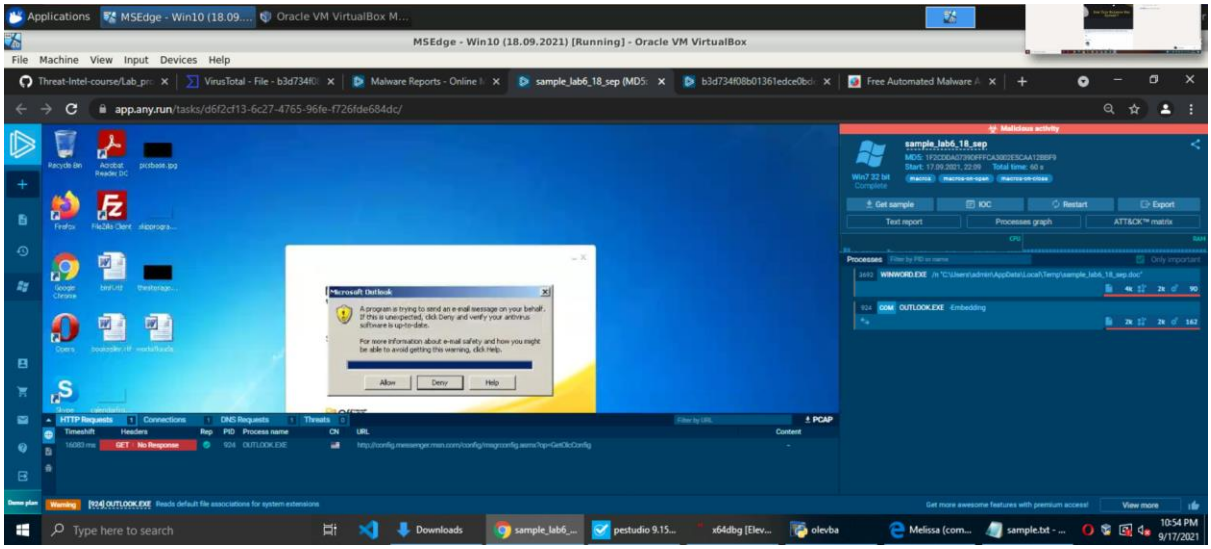
https://github.com/Vicky619git/ThreatIntelligence/blob/main/Malware%20Analysis/Melissa/OLEVBA%20Output/sample_melissa.txt

ANYRUN:


MSEdge - Win10 (18.09.2021) [Running] - Oracle VM VirtualBox
app.any.run/tasks/d6f2cf13-6c27-4765-96fe-f726fde684dc/
Microsoft
Word 2010
Starting.


MSEdge - Win10 (18.09.2021) [Running] - Oracle VM VirtualBox
app.any.run/tasks/d6f2cf13-6c27-4765-96fe-f726fde684dc/
Microsoft Outlook
The profile name is not valid. Enter a valid profile name.
OK
Cancel





MELISSA :

Melissa spreads via e-mail and by infecting Word documents and templates. The worm works in both, Office 97 (Word 8) and Office 2K (Word 9.0) and it uses Outlook to spread through e-mail.

The virus comes in .DOC formation, and attempts to replicate and send itself to other computers via email addresses on the computer. A variant of the virus also attempts to delete files. The user receives an email titled “My Pictures” which is blank but contains an attached file. When opened, it deletes data and sends itself to the first 0 entries in a person’s email address list.

Though the Melissa virus can be a problem, many people with newer forms of Word or Outlook have no problem with the worm type virus. It doesn't work on Word 2003, 2004, 2007. It is also called a macro virus, because it uses macro language. Most virus detectors will tell you if a program contains macros before you open it, so you can decide whether or not you should. You can also disable opening macros or documents that contain them on most computers.

Infection Process:

When an infected document is open, and the virus identifies the environment as Word 9.0, it removes the menu option 'Macro\Security' from the toolbar and enables all macros by directly modifying security settings in the registry: HKCU \Software\Microsoft\Office\9.0\Word\Security

Then the virus infects the Normal template. It checks if the first-class module is not called Melissa, then it removes any code from that module, replacing it with the virus code. If the virus runs from an infected Normal template, the virus uses the same method to infect the active document.

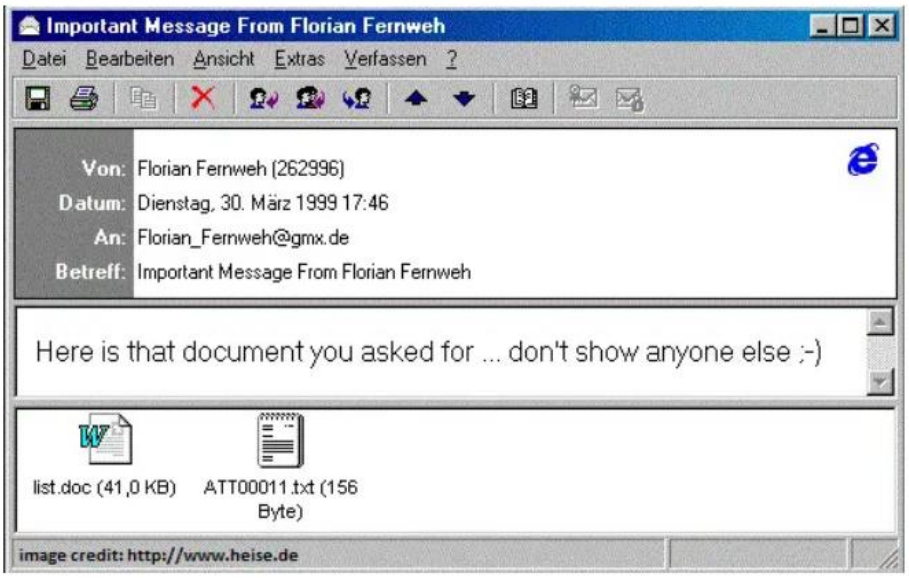
Next, the worm attempts to send itself out as an e-mail attachment. Since the mailing process is triggered once per each infected machine, the virus checks for the presence of its marker in the registry by comparing the value: HKCU\Software\Microsoft\Office\Melissa? against the string: "... by Kwyjibo".

If the above match is not found, and Outlook is installed on the system, the virus checks the Outlook address lists and collects up to 50 e-mail addresses from each list. It constructs the following e-mails (one per list):

Subject: Important Message From <user name>

Message: Here is that document you asked for ... don't show anyone else ;-)

Attachment: <currently open infected document>



(Image Source: https://cyberhoot.com/cybrary/melissa-virus/)

After the mailing process is completed, the virus sets the aforementioned marker (HKCU\Software\Microsoft\Office\Melissa? = “... by Kwyjibo") and moves on to infecting the Normal template.

Payload:

The virus checks the current time and date. If the number of minutes is equal to a day of a month, the virus inserts the following text into the open document:

"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

Addition Information:

The virus code contains the following comments:

WORD/Melissa written by Kwyjibo

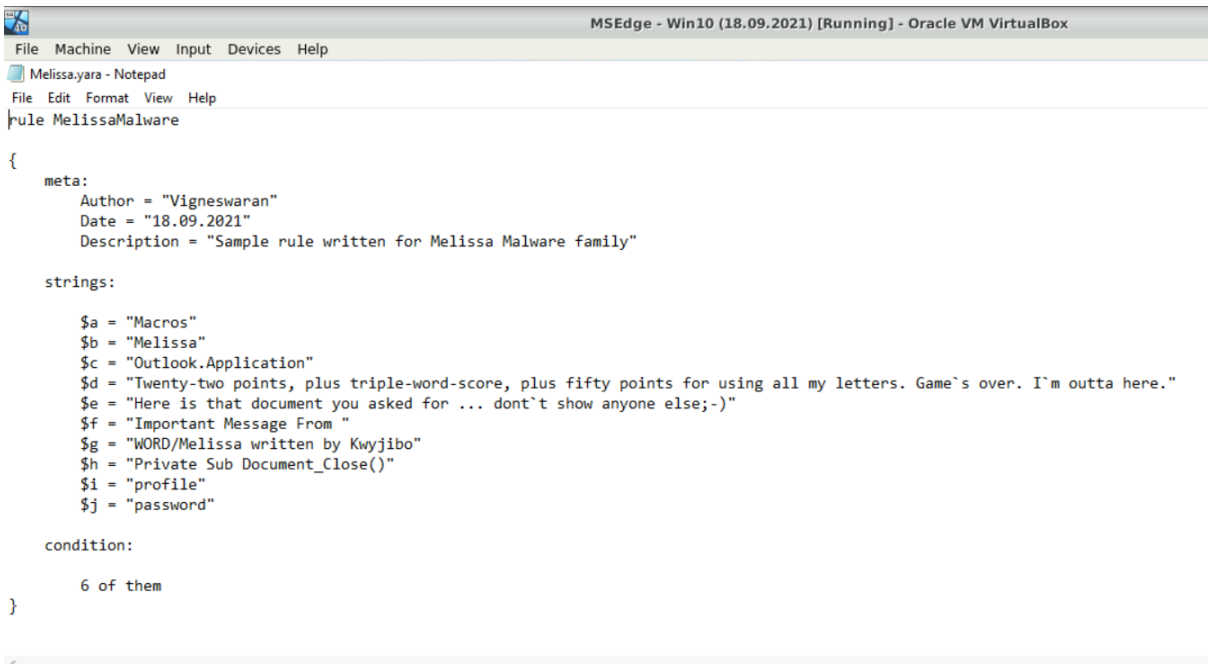
Works in both Word 2000 and Word 97

Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

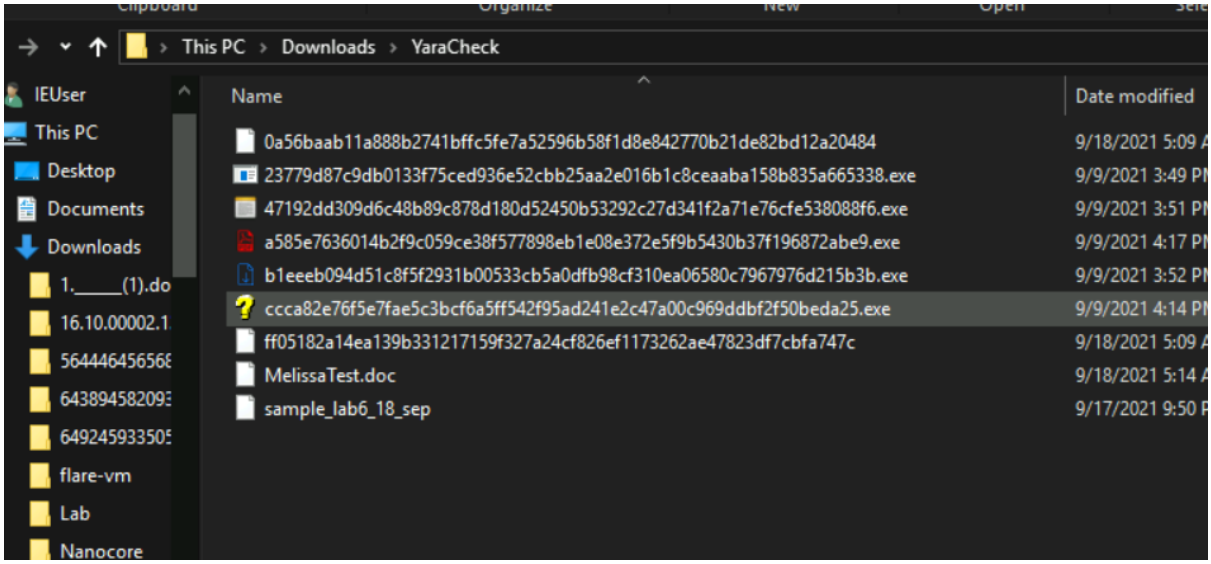
Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

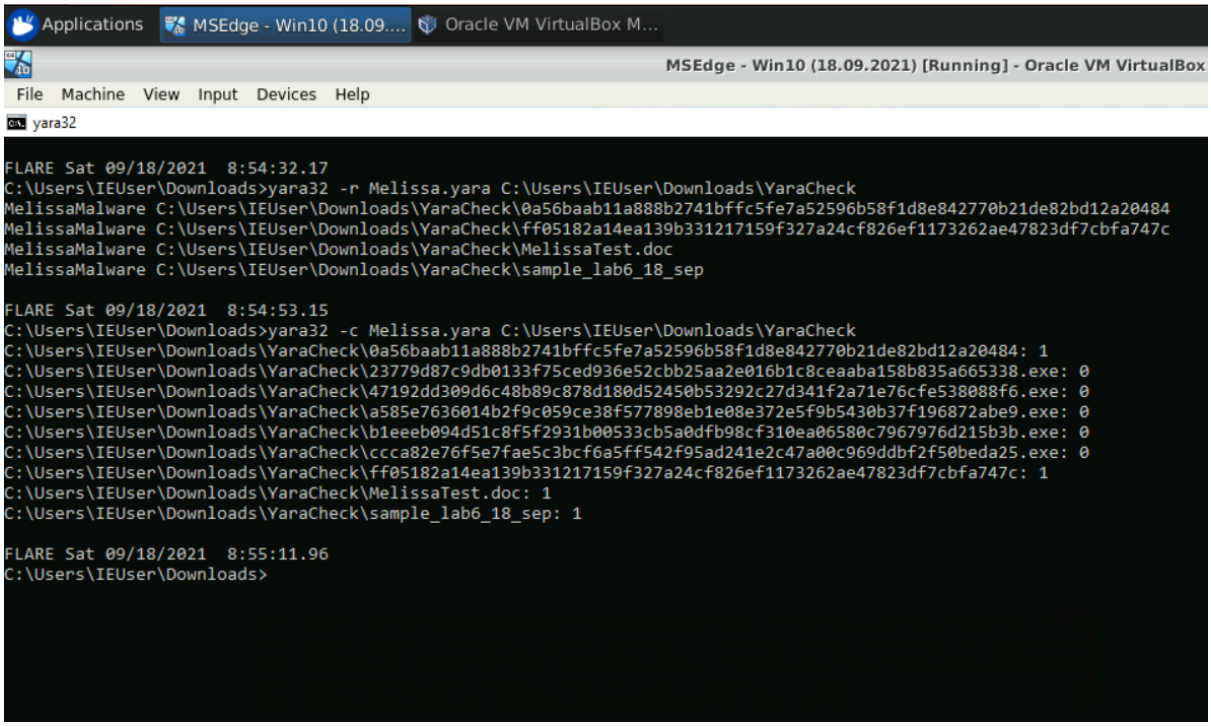
The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;).”

YARA RULE:




```
rule MelissaMalware

{
    meta:
        Author = "Vigneswaran"
        Date = "18.09.2021"
        Description = "Sample rule written for Melissa Malware family"

    strings:

        $a = "Macros"
        $b = "Melissa"
        $c = "Outlook.Application"
        $d = "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game`s over. I`m outta here."
        $e = "Here is that document you asked for ... dont`t show anyone else;-)"
        $f = "Important Message From "
        $g = "WORD/Melissa written by Kwyjibo"
        $h = "Private Sub Document_Close()"
        $i = "profile"
        $j = "password"

    condition:

        6 of them
}
```





References:

1. https://www.f-secure.com/v-descs/melissa.shtml
2. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus%3AW97M%2FMelissa.A
3. https://cyberhoot.com/cybrary/melissa-virus/