REPORT ON MELISSA VIRUS

PRESENTED BY

SUBHAN GHOSH MT20ACS539

Contents

Introduction

The Melissa virus was a mass-mailing macro virus released on or around March 26, 1999. It was reportedly named by Smith for a stripper in Florida, started by taking over victims' Microsoft Word program disabling a number of safeguards in Word 97 or Word 2000. It then used a macro to hijack their Microsoft Outlook email system and send messages to the first 50 addresses in their mailing lists. Those messages, in turn, tempted recipients to open a virus-laden attachment by giving it such names as "sexxxy.jpg" or "naked wife" or by deceitfully asserting, "Here is the document you requested ... don't show anyone else ;-)."

Technical Details

Melissa works with Microsoft Word 97, Microsoft Word 2000, and Microsoft Outlook 97 or 98 email client. One doesn't need to have Microsoft Outlook to receive the virus in email, but it will not spread itself further without it.

Melissa will not work under Word 95 and will not spread further under Outlook Express.

Melissa can infect Windows 95, 98, NT and Macintosh users. If the infected machine does not have Outlook or internet access at all, the virus will continue to spread locally within the user's own documents.

Propagation

Melissa arrives in an attachment to an e-mail note with the subject line "Important Message from [the name of someone]," and body text that reads "Here is that document you asked for...don't show anyone else ;-)". The attachment is often named LIST.DOC. If the recipient clicks on or otherwise opens the attachment, the infecting file is read to computer storage. The file itself originated in an Internet alt.sex newsgroup and contains a list of passwords for various Web sites that require memberships. The file also contains a Visual Basic script that copies the virus-infected file into the normal.dot template file used by Word for custom settings and default macros. It also creates this entry in the Windows registry:

HKEY_CURRENT_USERSoftwareMicrosoftOffice"Melissa?"="...by Kwyjibo"

The virus then creates an Outlook object using the Visual Basic code, reads the first 50 names in each Outlook Global Address Book, and sends each the same e-mail note with virus attachment that caused this particular infection. The virus only works with Outlook, not Outlook Express.

The email looked like this:

- From: (name of infected user)
- Subject: Important Message From (name of infected user)
- To: (50 names from alias list)
- Body: Here is that document you asked for ... don't show anyone else ;-)
- Attachment: LIST.DOC

We must remember that Melissa can arrive in any document, not necessarily just in this LIST.DOC where it was spread initially.

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

Infection

After sending itself out, the virus continues to infect other Word documents. Eventually, these files can end up being mailed to other users as well. This can be potentially disastrous, as a user might inadvertently send out confidential data to outsiders.

The virus activates if it is executed when the minutes of the hour match the day of the month; for example, 18:27 on the 27th day of a month. At this time the virus will insert the following payload of text into the current open document in Word:

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

This text, as well as the alias name of the author of the virus, "Kwyjibo", are all references to the popular cartoon TV series called "The Simpsons".

Impact

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.

The collective damage was enormous: an estimated $80 million for the cleanup and repair of affected computer systems.

Different Variants

- **Melissa.A** – First Variant
- **Melissa.I** –
    - uses a random number to select subject lines and message bodies of outgoing messages from eight different alternatives.
    - uses a different registry key (called "Empirical") to check whenever mass mailing has been done
    - contains an additional payload as well

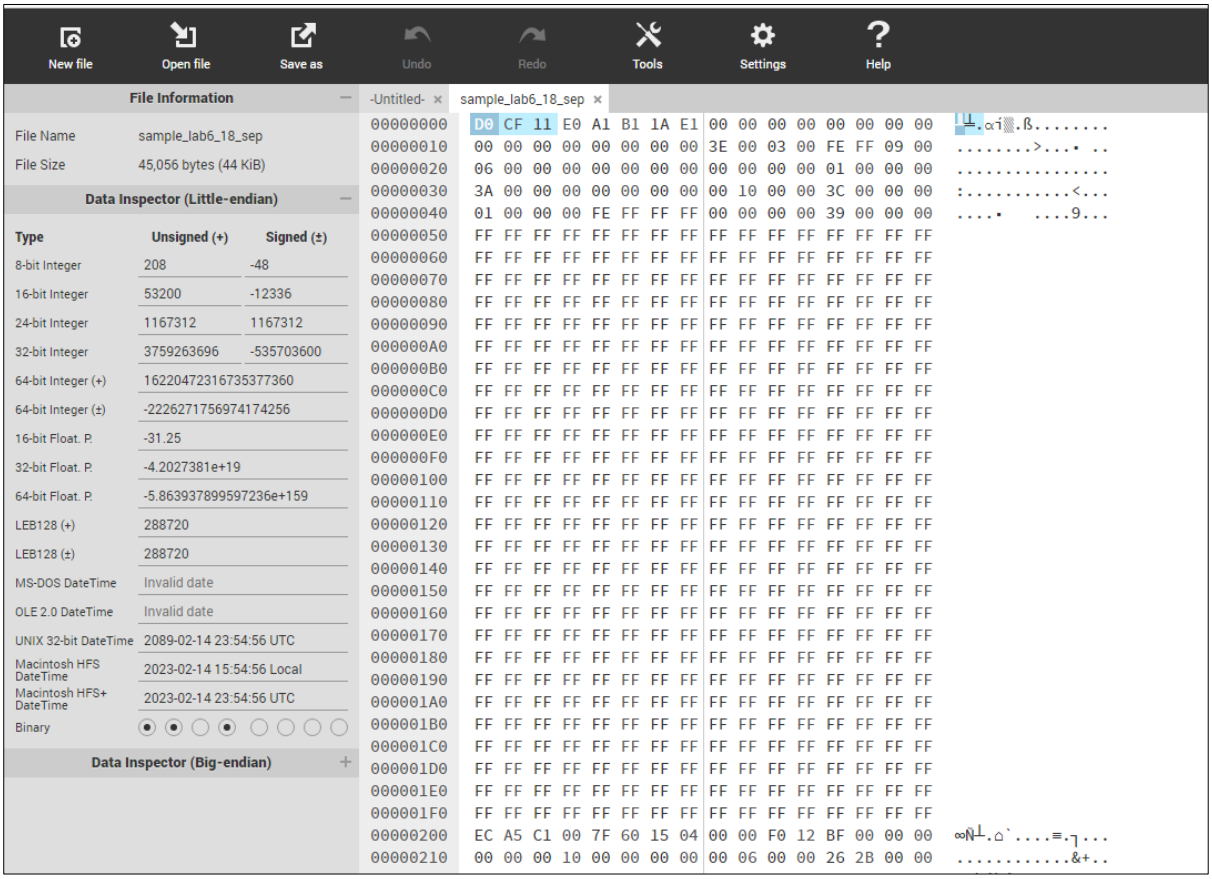
- **Melissa.O** – sends itself to 100 recipients from each Outlook address book.
- **Melissa.U** – uses the module name "Mmmmmmm" and it has a destructive payload.
- **Melissa.V** – sends itself to 40 recipients and the message is different.
- **Melissa.W** – does not lower macro security settings in Word 2000
- **Melissa.AO** – uses Outlook to send email message and the payload activates at 10 am on 10th day of each month.

How to Avoid Melissa

If you get an e-mail note with the subject, "Important Message from [the name of someone]," and it has an e-mail attachment (usually a 40-kilobyte document named LIST.DOC), simply DO NOT OPEN (for example, do not click on) the attachment. Write down the e-mail address of the person it came from. Delete the message. Then send a note to the sender so that they know that their computer has been infected.

Checking Type of File

Checked the file in hexed.it. Below is the snapshot of the webpage :

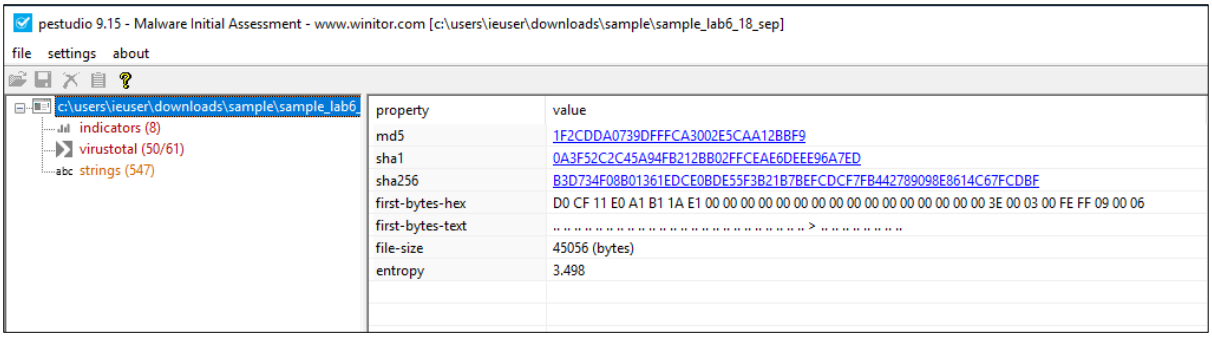


Validating file signature from Wikipedia file signature scheme:

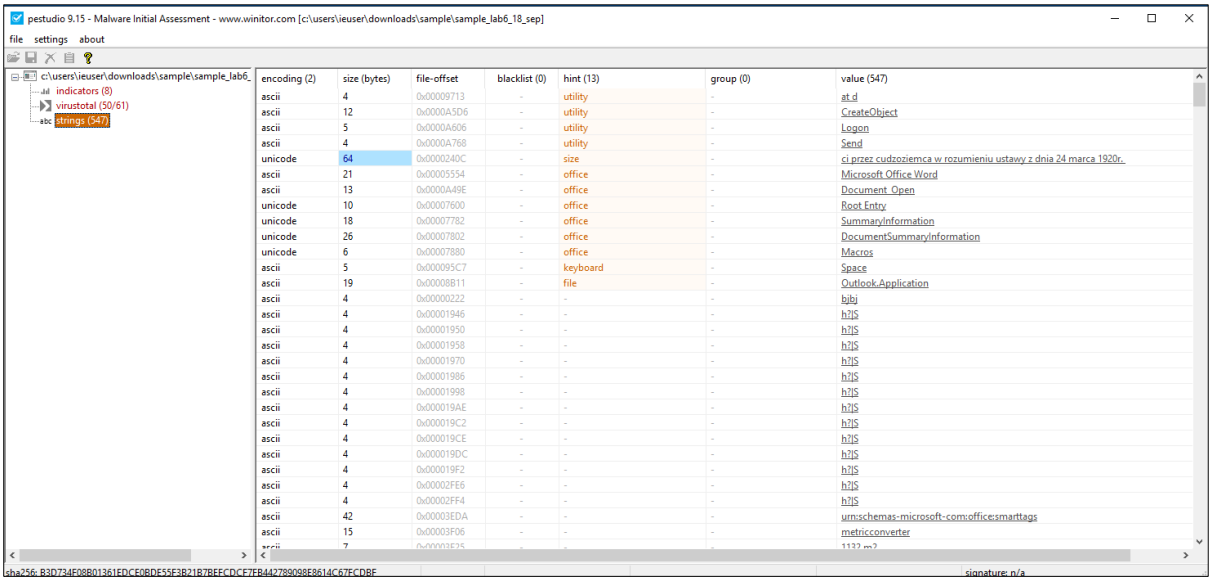
D0 CF 11 E0 A1 B1 1A E1	ÐÏ DC1 à ¡ ± SUB á	0	doc xls ppt msg	Compound File Binary Format, a container format used for document by older versions of Microsoft Office.[27] It is however an open format used by other programs as well.

Static Analysis using PEStudio

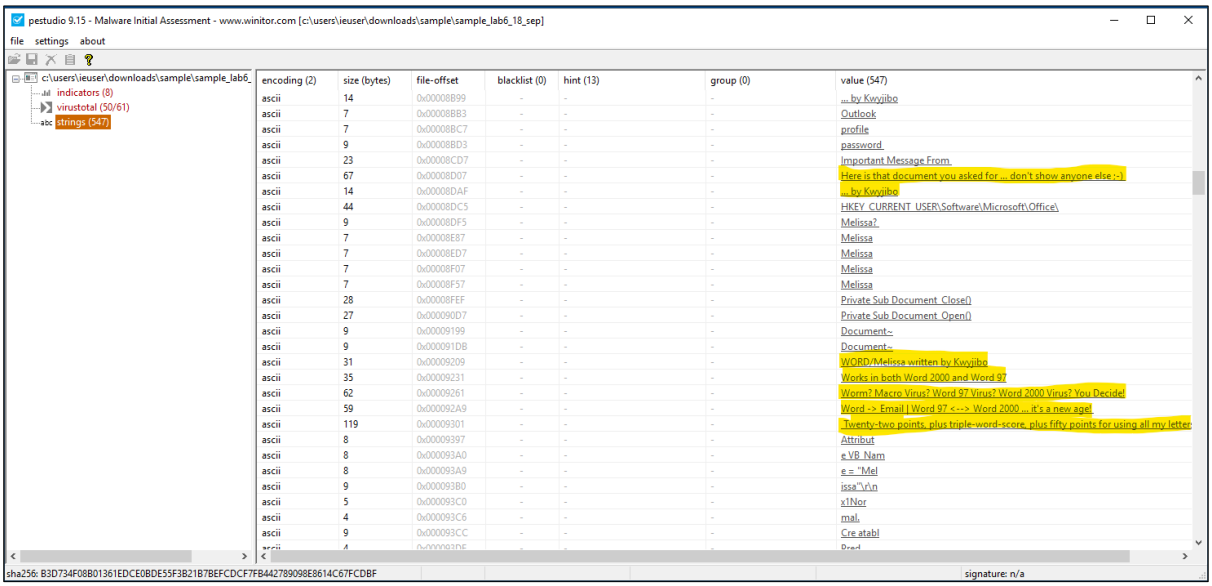
Here we can see the Hash Values, first bytes and entropy of the sample file.



In this snapshot, we can confirm that the sample is Microsoft Office Word file.

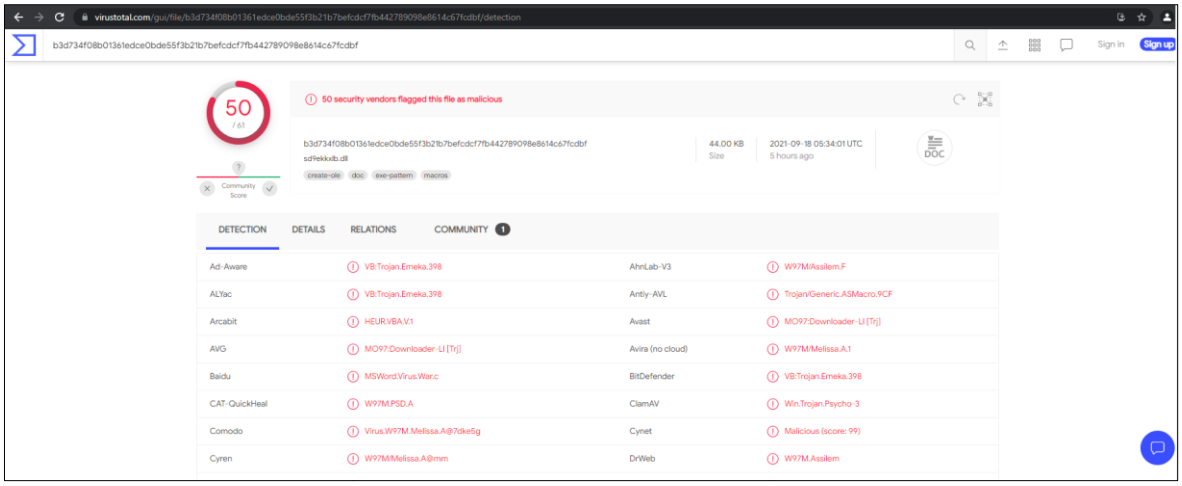


Here are few other strings which we are going to use while creating the Yara rule.

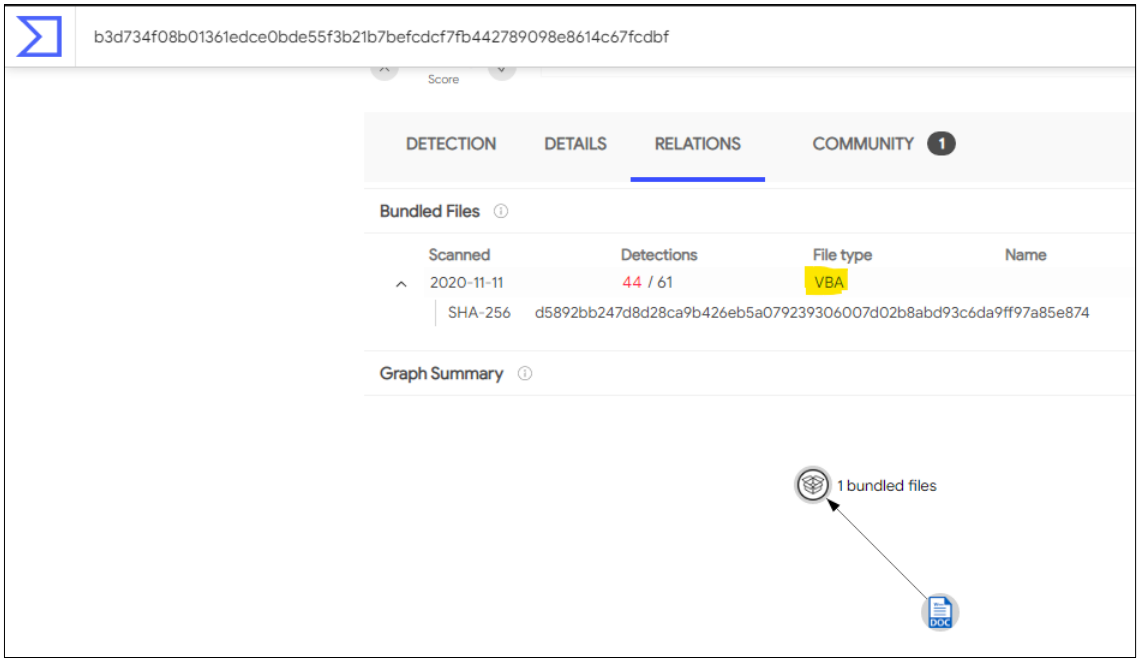


Static Analysis using VirusTotal

In the below snapshots, we can confirm the hash and file type.



In the below snapshots, we can confirm that the sample file is using embedded macro (bundled VBA file).

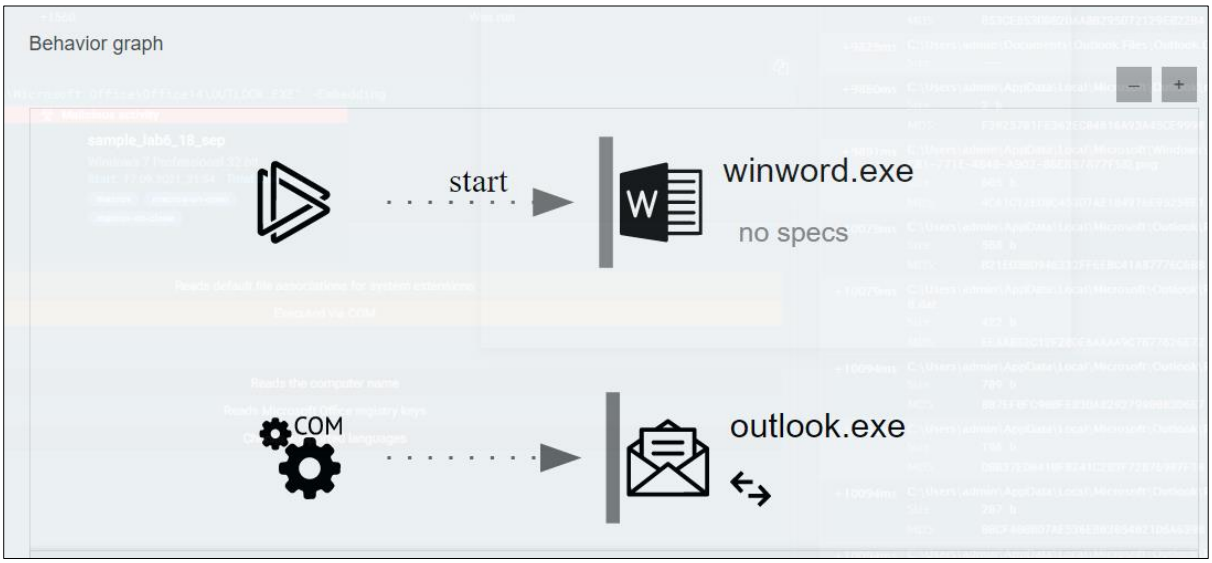


Dynamic Analysis using Any.Run

Ran the sample file under sandboxed environment (Under trial version for 1 minute). Below are few details from the website:

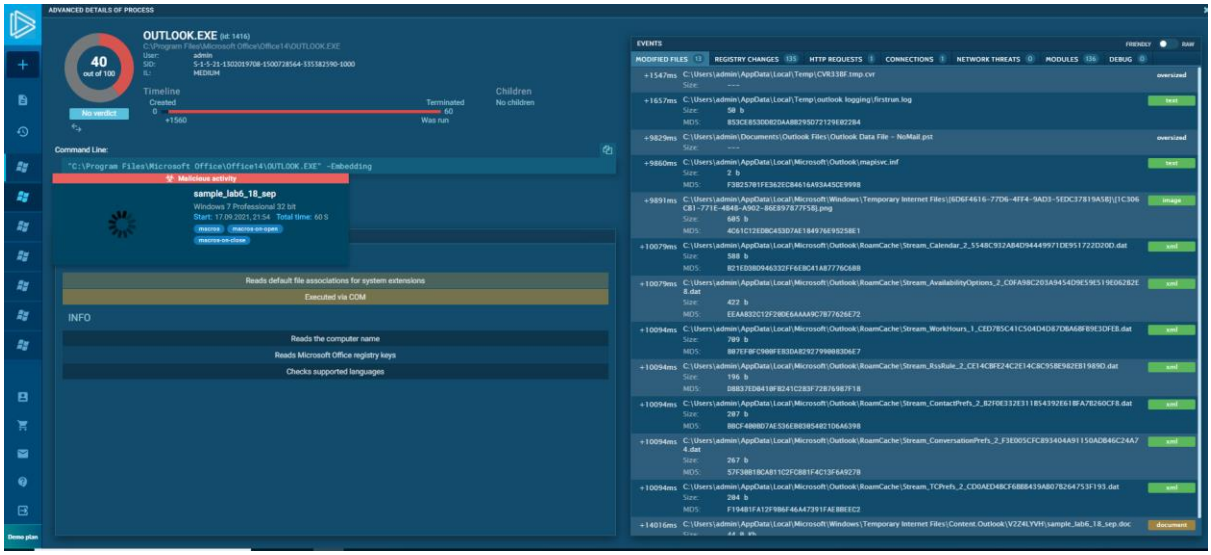
Behavior Graph

We can see that the word file is calling the embedded VBA macro script to open Outlook and then it will read the first 50 address in the address book and try to send the malicious code.



Process Graph

Here, it is clearly visible that the execution of outlook.exe has been listed as a warning and malicious activity.



Dropped Files

Dropped files

PID	Process	Filename	Type
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Temp\CVR33BF.tmp.cvr MD5: — SHA256: —	—
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\mapisvc.inf MD5: F3B25701FE362EC84616A93A45CE9998 SHA256: B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209	text
3596	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR2E41.tmp.cvr MD5: — SHA256: —	—
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\V2Z4LYVH\sample_lab6_18_sep.doc MD5: 1F2CDDA0739DFFFCA3002E5CAA12BB... SHA256: B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF	document
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ContactPrefs_2_B2F0E332E311B54392E61BFA7B260CF8.dat MD5: BBCF400BD7AE536EB03054021D6A6398 SHA256: 383020065C1F31F4FB09F448599A6D5E532C390AF4E5B8AF0771FE17A23222AD	xml
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ConversationPrefs_2_F3E005CFC893404A91150ADB46C24A74.dat MD5: 57F30B1BCA811C2FCB81F4C13F6A927B SHA256: 612BAD93621991CB09C347FF01EC600B46617247D5C041311FF459E247D8C2D3	xml
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_WorkHours_1_CED7B5C41C504D4D87DBA6BFB9E3DFEB.dat MD5: 807EF0FC900FEB3DA82927990083D6E7 SHA256: 4411E7DC9780112227649430815 00FFF0E43CBF7CCD44264BD1AB6306CA68913	xml
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_AvailabilityOptions_2_C0FA98C203A9454D9E59E519E062B2E8.dat MD5: EEAA832C12F20DE6AAAA9C7B77626E72 SHA256: C4C9A90F2C961D9EE79CF08FBEE647ED7DE0202288E876C7BAAD00F4CA29CA16	xml
1416	OUTLOOK.EXE	C:\Users\admin\Documents\Outlook Files\Outlook Data File - NoMail.pst MD5: — SHA256: —	—
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_Calendar_2_5548C932AB4D94449971DE951722D20D.dat MD5: B21ED3BD946332FF6EBC41A87776C6BB SHA256: B1AAC4E817CD10670B785EF8E5523C4A883F44138E50486987DC73054A46F6F4	xml
3596	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd MD5: 6E3B7226F8E54D42D2143FA836C2BFEB SHA256: 24039B2A80386AFDD57EE1301B5AC5629A6EE144C284F8AE323BA257CC3E8132	tlb
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Temp\outlook logging\firstrun.log MD5: 853CE853DD82DAA8B295D72129E022B4 SHA256: E4BF8FD5E1E40D86D6599C9149DAD08C90DDC3D8CA8A50A7A419F4F7DE58A901	text
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\{6D6F4616-77D6-4FF4-9AD3-5EDC37819A5B}\{1C306CB1-771E-4B4B-A902-86E897877F5B}.png MD5: 4C61C12EDBC453D7AE184976E95258E1 SHA256: 296526F9A716C1AA91BA5D6F69F0EB92FDF79C2CB2CFCF0CEB22B7CCBC27035F	image
3596	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	pgc

Below is the execution report and full analysis link of ANY.RUN website:

[b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf | ANY.RUN - Free Malware Sandbox Online]

Dynamic Analysis using Olevba

Execution report generated through dynamic analysis of the malware sample selected by olevba tool in flare VM environment (Full Report attached in GitHub):

```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Close      |Runs when the Word document is closed        |
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|sample              |May detect Anubis Sandbox                    |
|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             |
+----------+--------------------+---------------------------------------------+
```

Below is the full report from InQuest Lab Deep File Inspection (DFI):
https://labs.inquest.net/dfi/hash/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

YARA Rule Execution

Yara Rule has been uploaded in GitHub (https://github.com/subhanghosh/ThreatIntelligenceLab/blob/main/LAB6-Melissa/melissa.yar)

Below is the execution in flare VM with samples:

```
FLARE Sat 09/18/2021  4:09:02.72
C:\Users\IEUser\Desktop>yara32 C:\Users\IEUser\Desktop\melissa.yar C:\Users\IEUser\Downloads\sample
Melissa C:\Users\IEUser\Downloads\sample\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
Melissa C:\Users\IEUser\Downloads\sample\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
Melissa C:\Users\IEUser\Downloads\sample\sample_lab6_18_sep
```

Reference

1) https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519
2) https://searchsecurity.techtarget.com/definition/Melissa-virus
3) https://www.f-secure.com/v-descs/melissa.shtml