**Melissa Malware Analysis**

## Description of Virus:

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. It targeted Microsoft Word and Outlook-based systems and created considerable network traffic. 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 ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first fifty people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.

## VirusTotal analysis:

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

**Type of File** = MS Word Document

**MD5**: 1f2cdda0739dfffca3002e5caa12bbf9

**SHA1**: 0a3f52c2c45a94fb212bb02ffceae6deee96a7ed

**SHA256**: b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

**SHA512**: 227f0a8942af2073516a616a0518a8c7be9a84b168b92d4e7d054d99e19fc3ace4b4e26c0e33f7f1df8016fa77ef34264872a99e3c4e3f8ed84951d6143313cf

**Size**: 45,056B

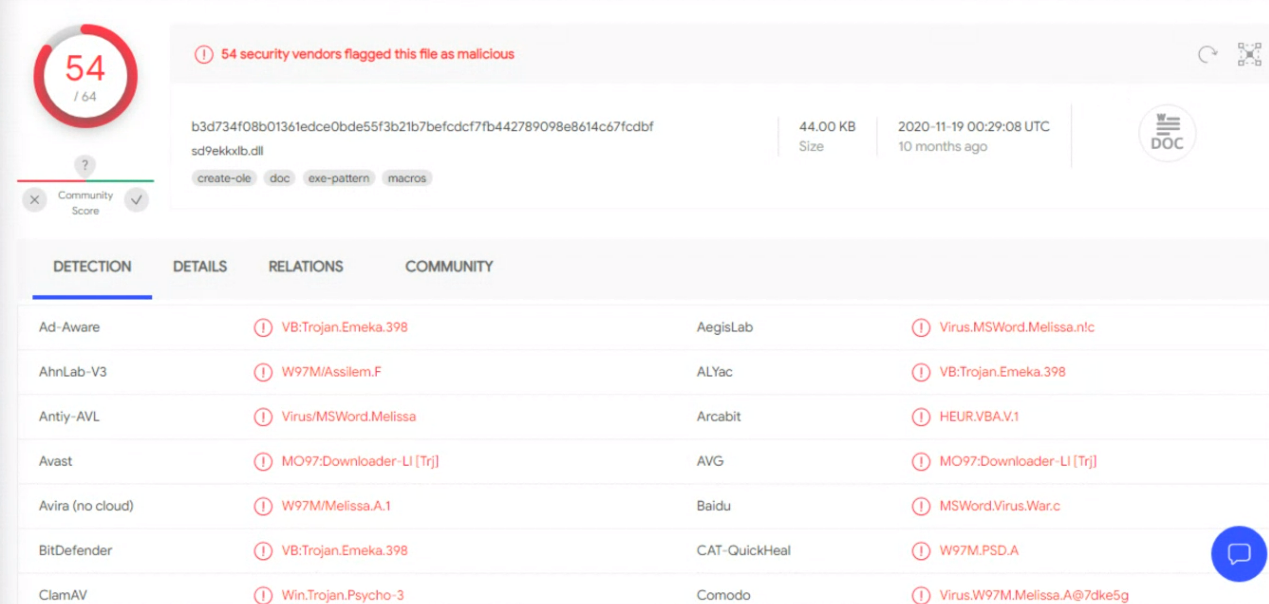


Fig1

## Hex editor analysis of file



Fig2

## Olevba analysis

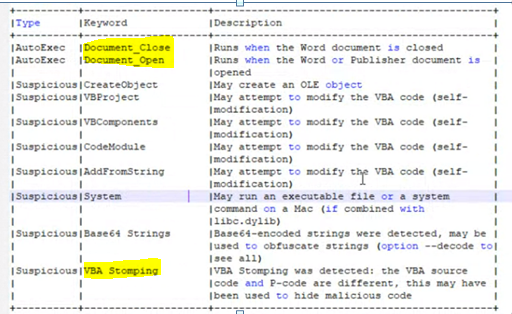


Fig3

Few Observations from above screenshot-

* Keywords Document\_Close and Document\_Open : Code is automatically getting executed on the open and close action 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-



Fig4

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.

## 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 Fig4)

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](https://whatis.techtarget.com/definition/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](https://whatis.techtarget.com/definition/registry):

HKEY\_CURRENT\_USERSoftwareMicrosoftOffice"Melissa?"="...by Kwyjibo"

1. The virus then creates an Outlook [object](https://searchapparchitecture.techtarget.com/definition/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.
2. The virus also disables some security safeguards.

## THREAT INTEL –

* The Melissa virus was a mass-mailing [macro virus](https://en.wikipedia.org/wiki/Macro_virus) released on or around March 26, 1999. As it was not a standalone program, it was not classified as a [worm](https://en.wikipedia.org/wiki/Computer_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.
* 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.

## YARA RULE-

rule Melissa\_Virus

{

meta:

description = "Mass-mailing macro virus"

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!"

condition:

all of ($var\*)

}