Lab-6

Melissa Macro Malware

Mohammad Faheemuddin

MT20ACS517

Contents

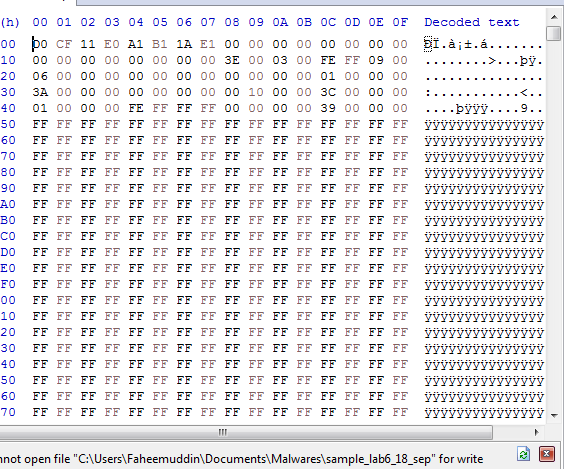
[Type of File 3](#_Toc82874513)

[About Melissa Virus- What the file does 3](#_Toc82874514)

[Static Analysis 4](#_Toc82874515)

# Type of File

The given file has header as D0 CF 11 E0 A1 B1 1A E1 which is An Object Linking and Embedding (OLE) Compound File (CF) (i.e., [OLECF](http://www.forensicswiki.org/wiki/OLE_Compound_File)) file format, known as Compound Binary File format by Microsoft, used by Microsoft Office 97-2003 applications (Word, PowerPoint, Excel, Wizard). Therefore, it is **MS Word Document File.**



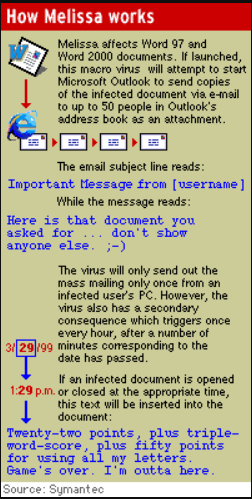
# About Melissa Virus- What the file does

Scanning the file on Virus Total provides details about the malware. The virus is Melissa Macro Virus.

The Melissa virus, reportedly named by Smith for a stripper in Florida, started by taking over victims’ Microsoft Word program. 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 ;-).”

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.

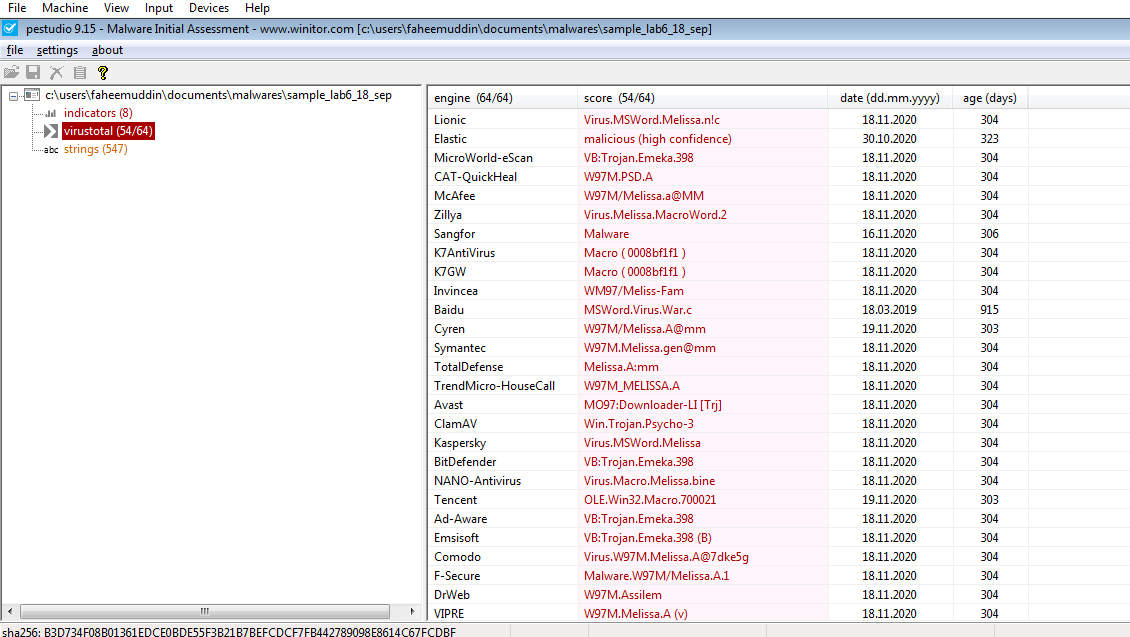
Within a few days, cybersecurity experts had mostly contained the spread of the virus and restored the functionality of their networks, although it took some time to remove the infections entirely. Still, the collective damage was enormous: an estimated $80 million for the cleanup and repair of affected computer systems.



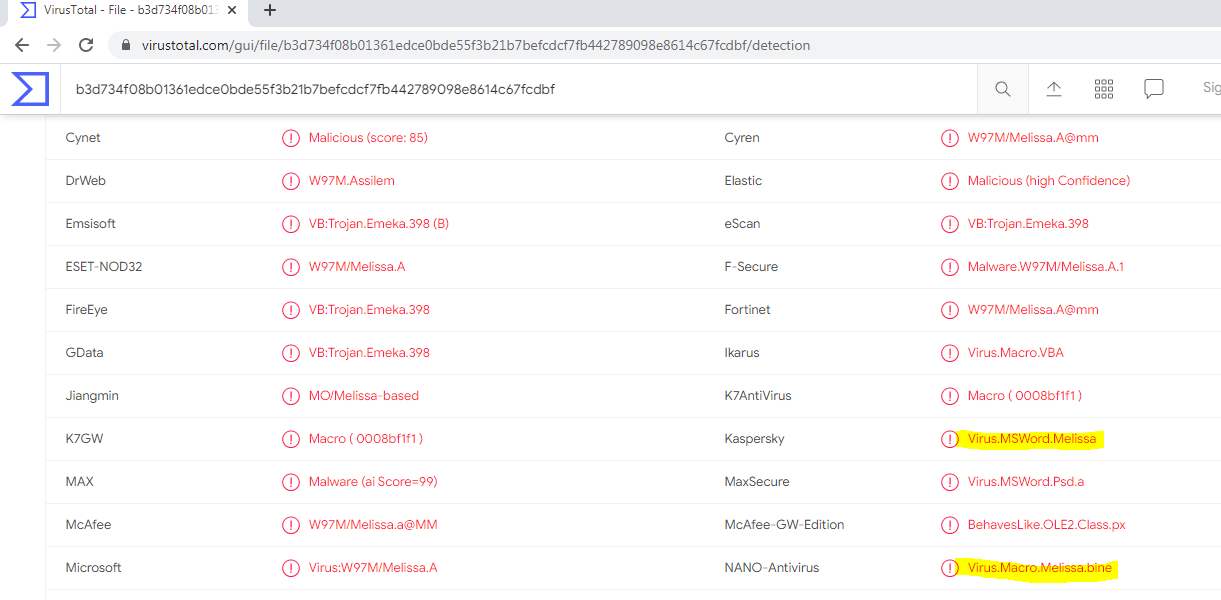
# Static Analysis

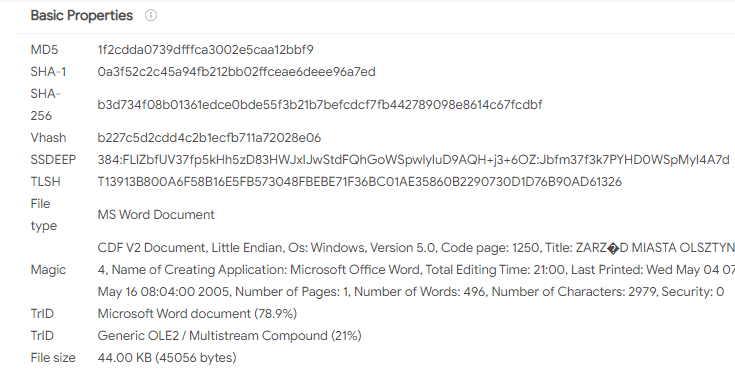
# Virus Total

**Reported Malicious by majority of the vendors 54/64**



Detected as Melissa Virus:





# Detected Strings in the sample

Send

Outlook.Application

Melissa

Outlook

profile

password

WORD/Melissa written by Kwyjibo

Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

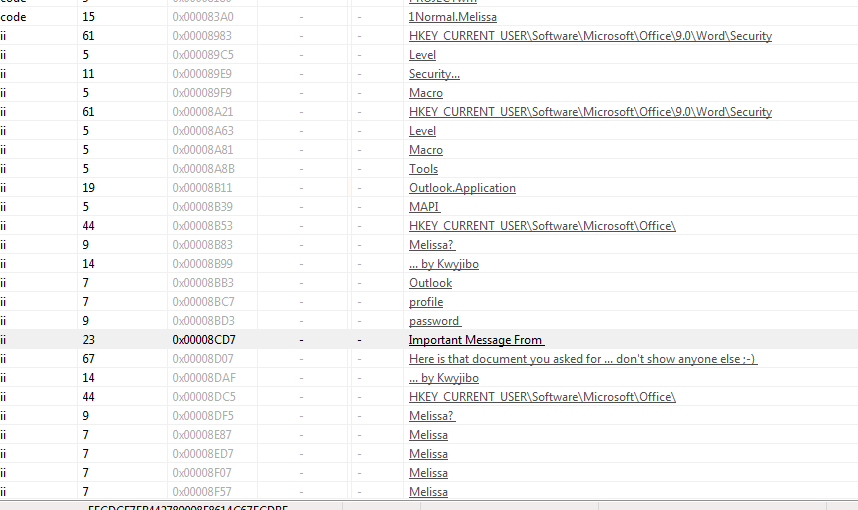
Word -> Email Word 97 <--> Word 2000 ... it's a new age!

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

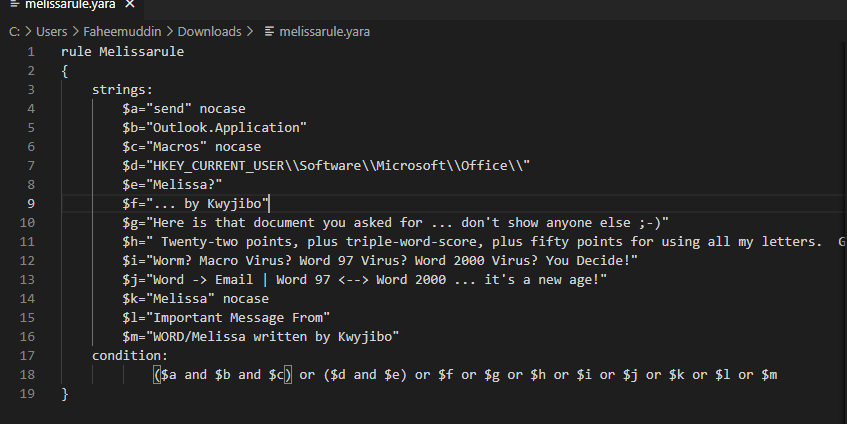
Important Message From

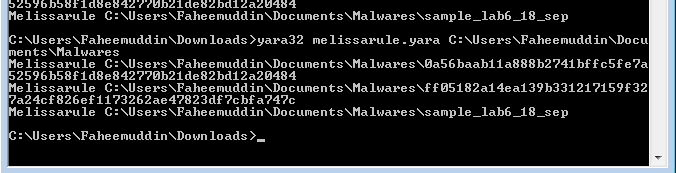
Here is that document you asked for ... don't show anyone else :-)

... by Kwyjibo



# Yara Rule





# Analysis using Oletools

The table shown in the image below contains an overview of what was found in the macro.

The information we are interested in the most is the Base64 encoded strings. Encoding with Base64 is a common technique used by malware authors to try and obfuscate their code and make it more difficult for anti-virus to detect.

Also it contains other AutoExec and suspicious type code.

