Malware Analysis Report

Table of Contents

[Overview : 1](#_Toc82918540)

[Melissa : 1](#_Toc82918541)

[History : 1](#_Toc82918542)

[Overview of the Malware : 1](#_Toc82918543)

[Malware Working Procedure : 2](#_Toc82918544)

[How to Avoid Melissa : 2](#_Toc82918545)

[Static Analysis: 3](#_Toc82918546)

[Dynamic Analysis: 10](#_Toc82918547)

[Yara rule : 13](#_Toc82918548)

[Reference : 13](#_Toc82918549)

# Overview :

This is the report on the sample we were provided in the lab 5. Malware analysis was done on the sample (both static and dynamic analysis). I have tried to do the analysis and found the family to be Melissa.

# Melissa :

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.

A programmer named David Lee Smith hijacked an America Online (AOL) account and used it to post a file on an Internet newsgroup. The posting promised dozens of free passwords to fee-based websites with adult content. When users took the bait, downloading the document and then opening it with Microsoft Word, a virus was unleashed on their computers.[1]

# History :

The Melissa virus, reportedly named by Smith 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 adult names or by deceitfully asserting, “Here is the document you requested ... don’t show anyone else ;-).” With the help of some devious social engineering, the virus operated like a sinister, automated chain letter.

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.

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.

# Overview of the Malware :

Melissa is a fast-spreading macro [virus](https://searchsecurity.techtarget.com/definition/virus) that is distributed as an e-mail attachment that, when opened, disables a number of safeguards in Word 97 or Word 2000, and, if the user has the Microsoft Outlook e-mail program, causes the virus to be resent to the first 50 people in each of the user's address books. While it does not destroy files or other resources, Melissa has the potential to disable corporate and other mail servers as the ripple of e-mail distribution becomes a much larger wave. On Friday, March 26, 1999, Melissa caused the Microsoft Corporation to shut down incoming e-mail

# Malware Working Procedure :

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](https://whatis.techtarget.com/definition/newsgroup) and contains a list of passwords for various Web sites that require memberships. The file also contains a Visual Basic [script](https://whatis.techtarget.com/definition/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](https://whatis.techtarget.com/definition/registry):

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

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. The virus only works with Outlook, not Outlook Express.

In a small percentage of cases (when the day of the month equals the minute value), a payload of text is written at the current cursor position that says:

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

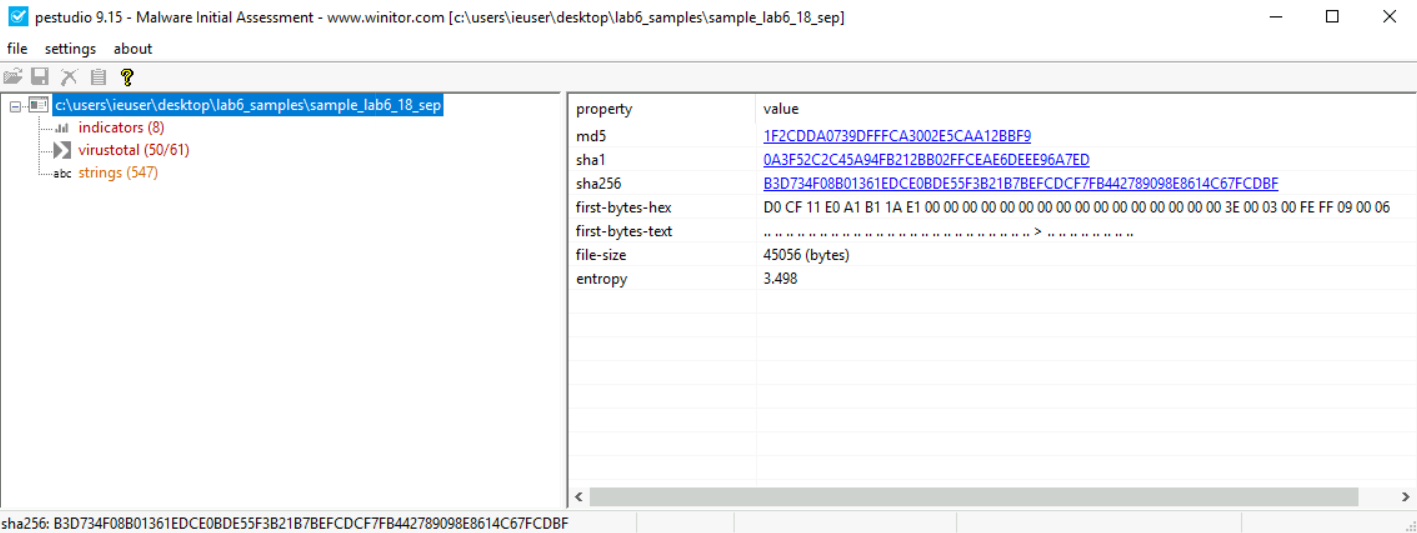
# How to Avoid Melissa :

Avoiding Melissa does not mean you can't read your e-mail - only that you have to screen your notes and be careful about what attachments you open.

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.

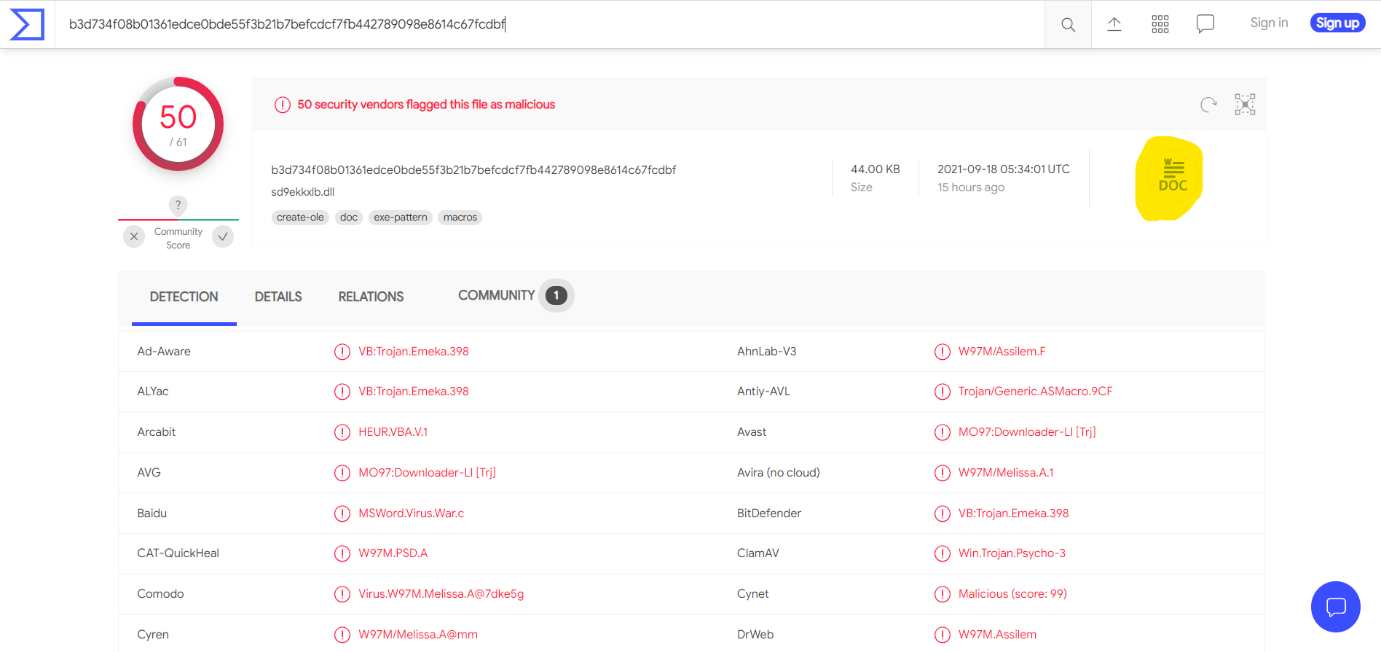
# Static Analysis:

For static analysis PEStudio, VirusTotal.com, OLEVBA tool are used. Basic information are revealed from PEStudio. Once it is found that it is Melissa which runs through a VB script in the doc file as part of a Macro, OLEVBA tool is used to do the further analysis and information gathering. String analysis was done from the PEStudio.



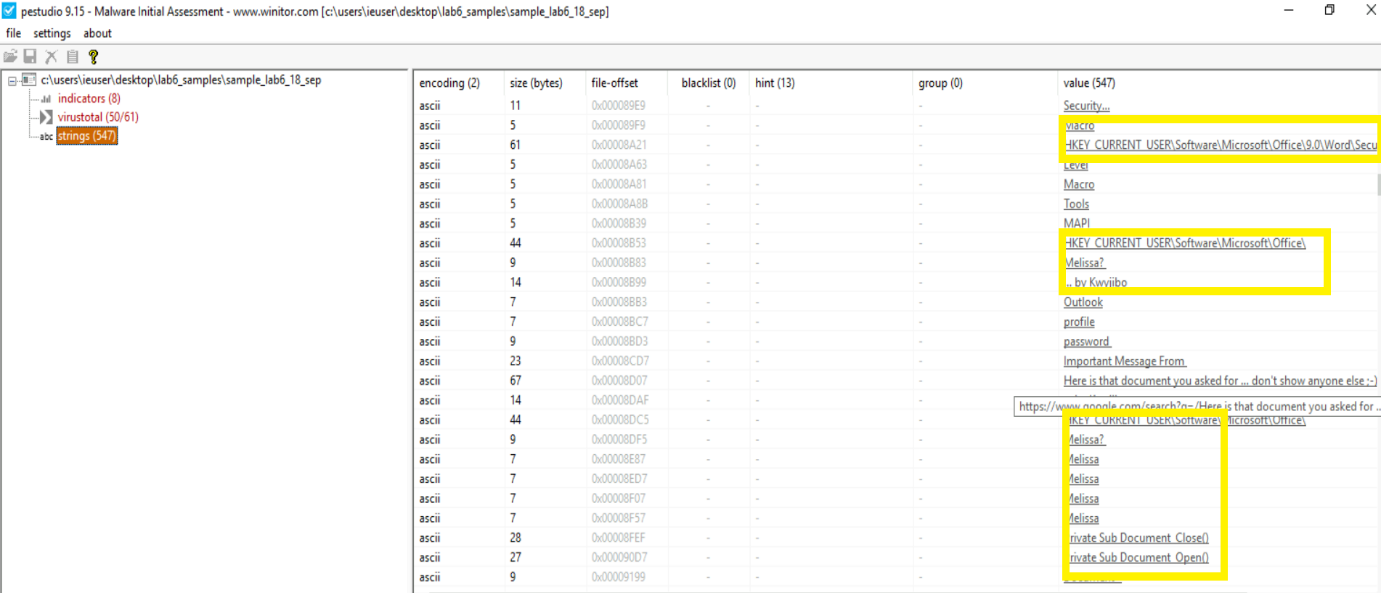
First byte-hex is D0 CF 11 E0 A1 which is the indicator that the signature scheme might match with doc/xls/ppt/msg.

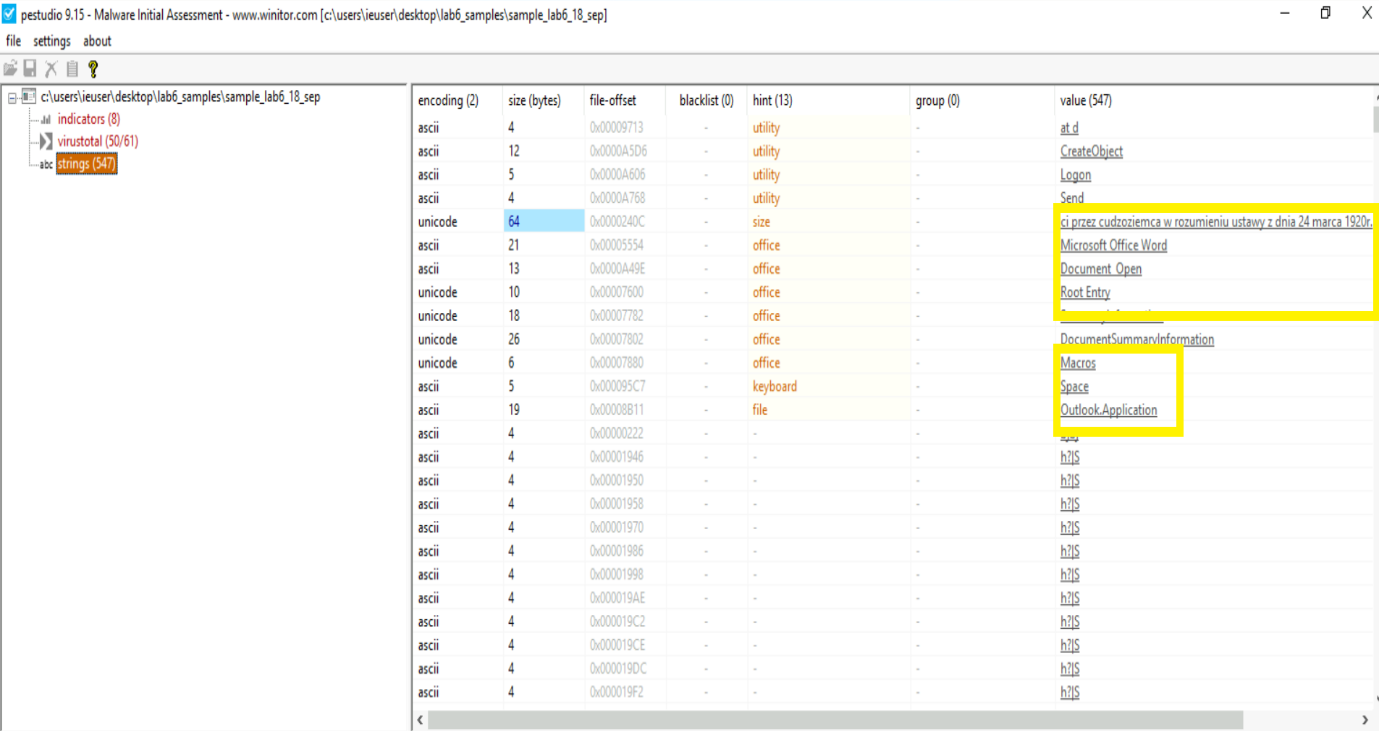
Further, I uploaded the sample to virustotal website to gather more info.

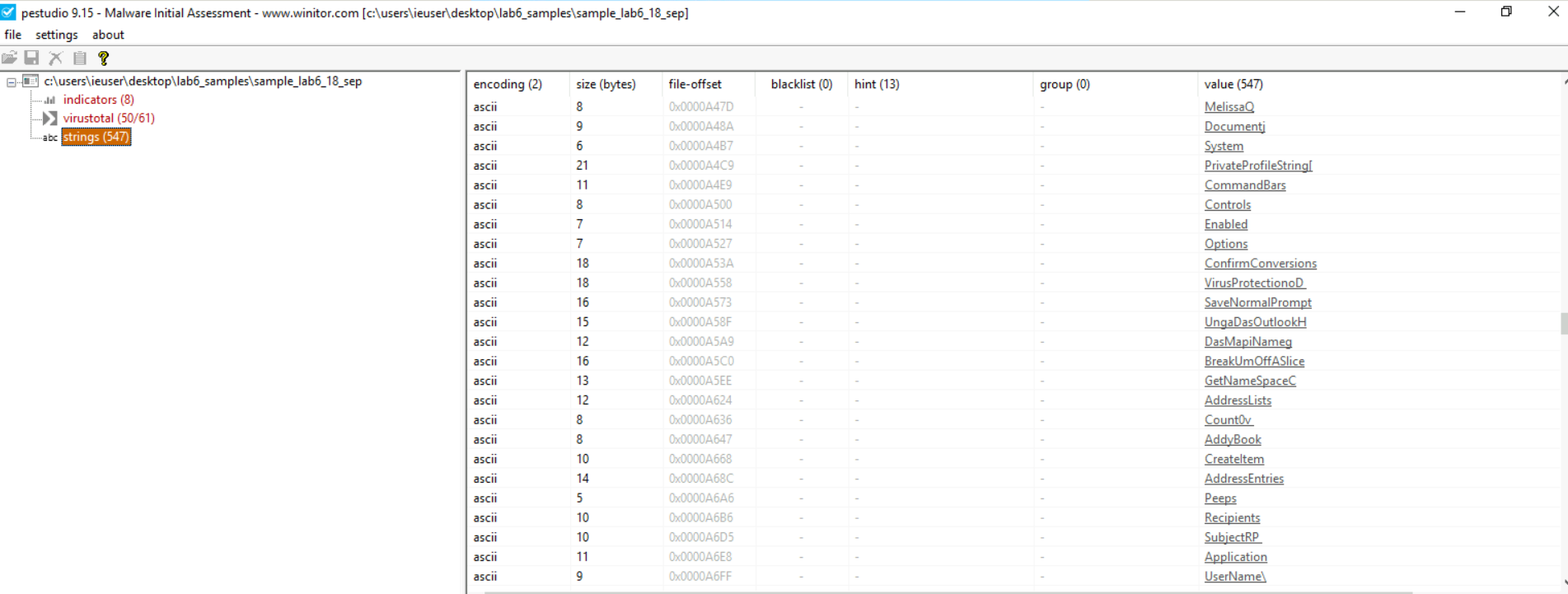


This indicated that it is a doc file.

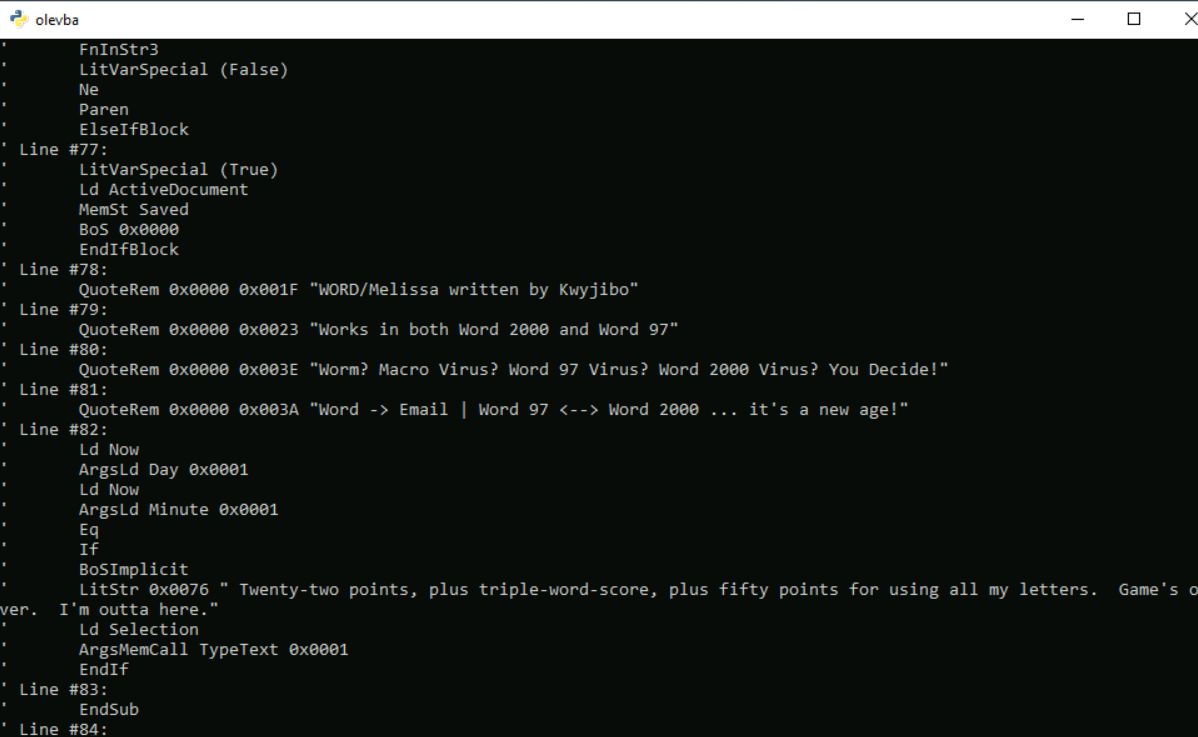
I checked the strings in PEStudio to understand the malware and its content. Below are some of the findings for Sample1.

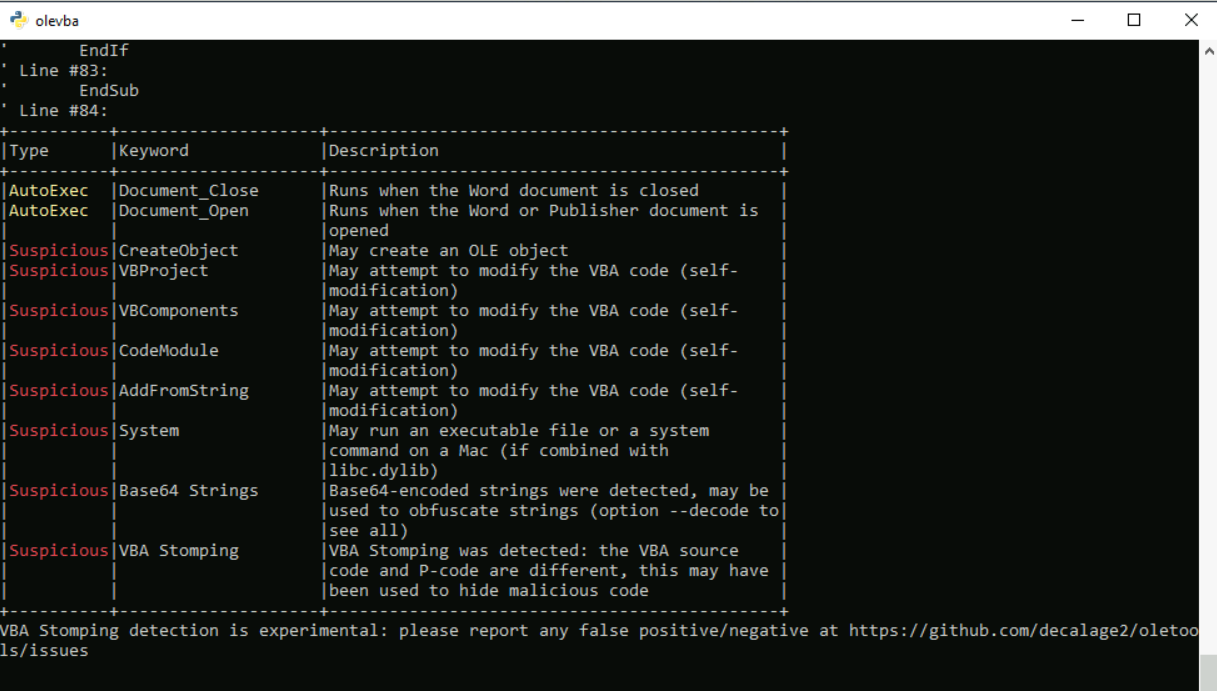






After getting the information about the Malware it was understood that it uses macro which is a part of doc file as VB script. So further analysis was done on OLEVBA tool



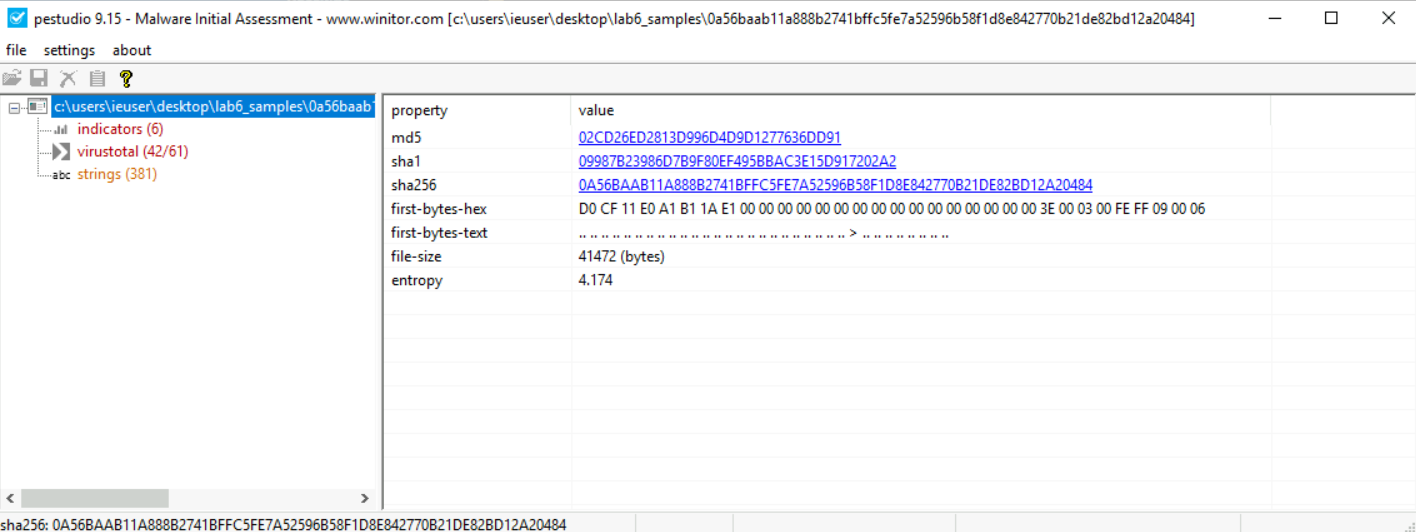


As we can clearly see here, 8 instructions are suspicious. Complete report of this OLEVBA tool is attached here.

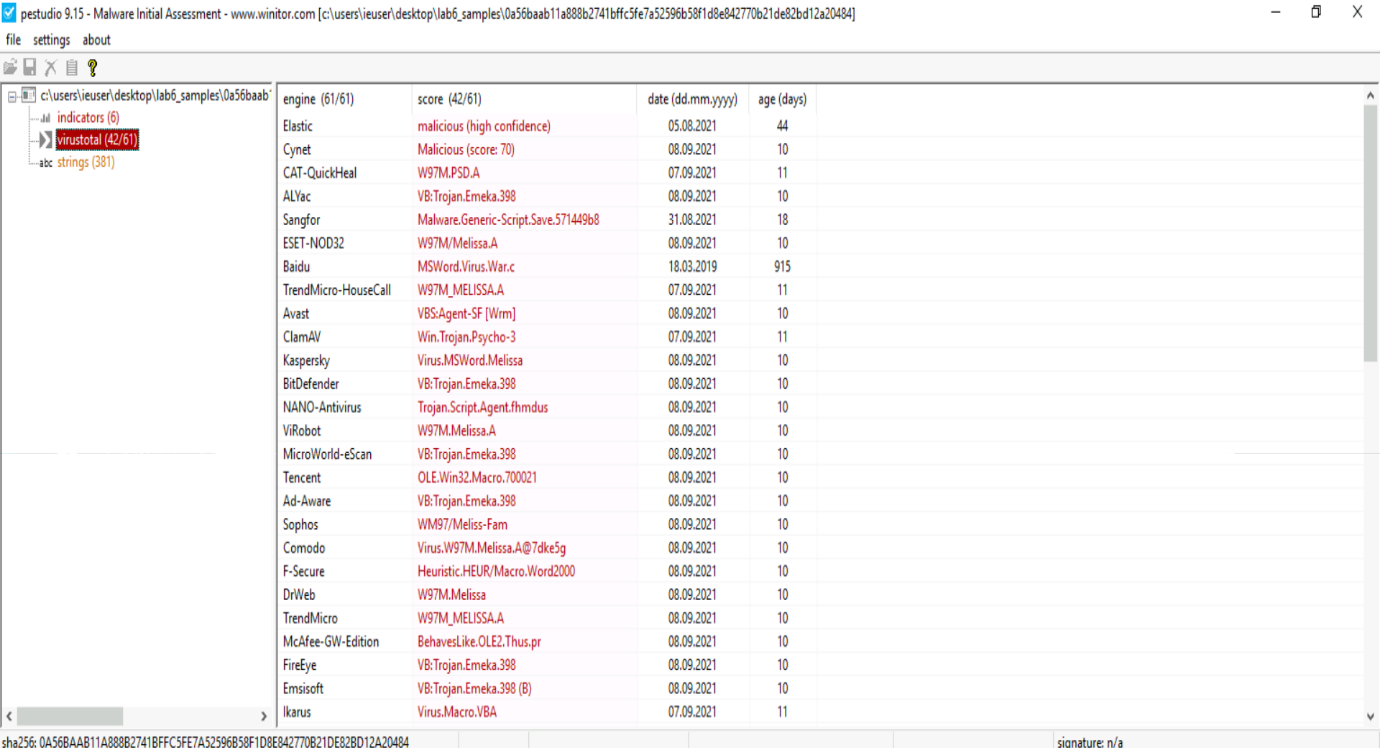


Further, we found out the similar samples to have a thorough understanding and detect a pattern.

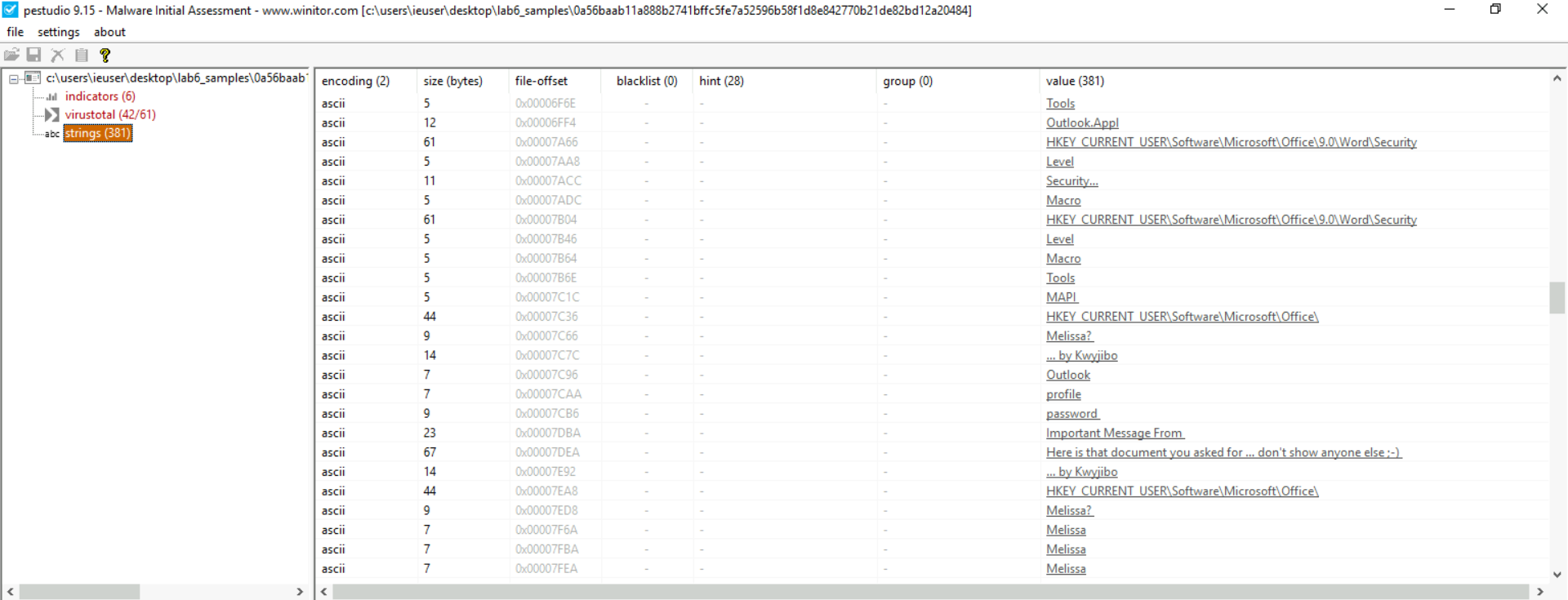
**For Sample 2**

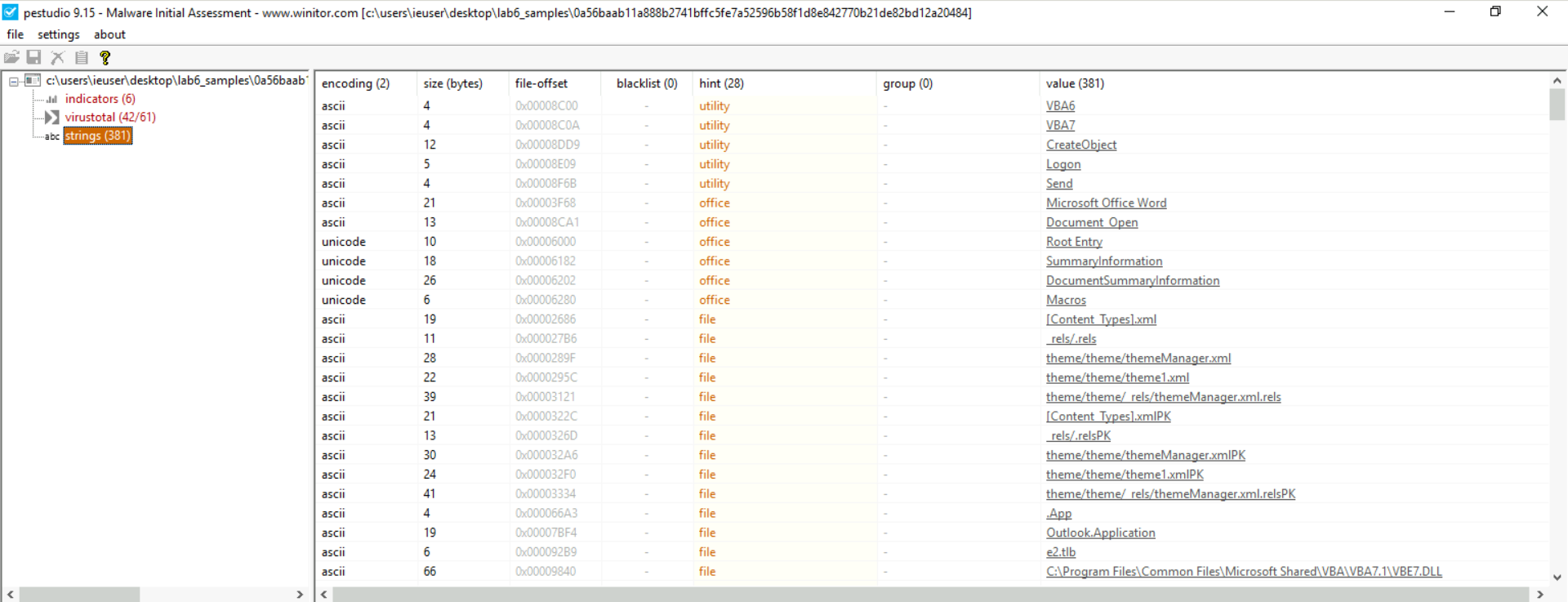


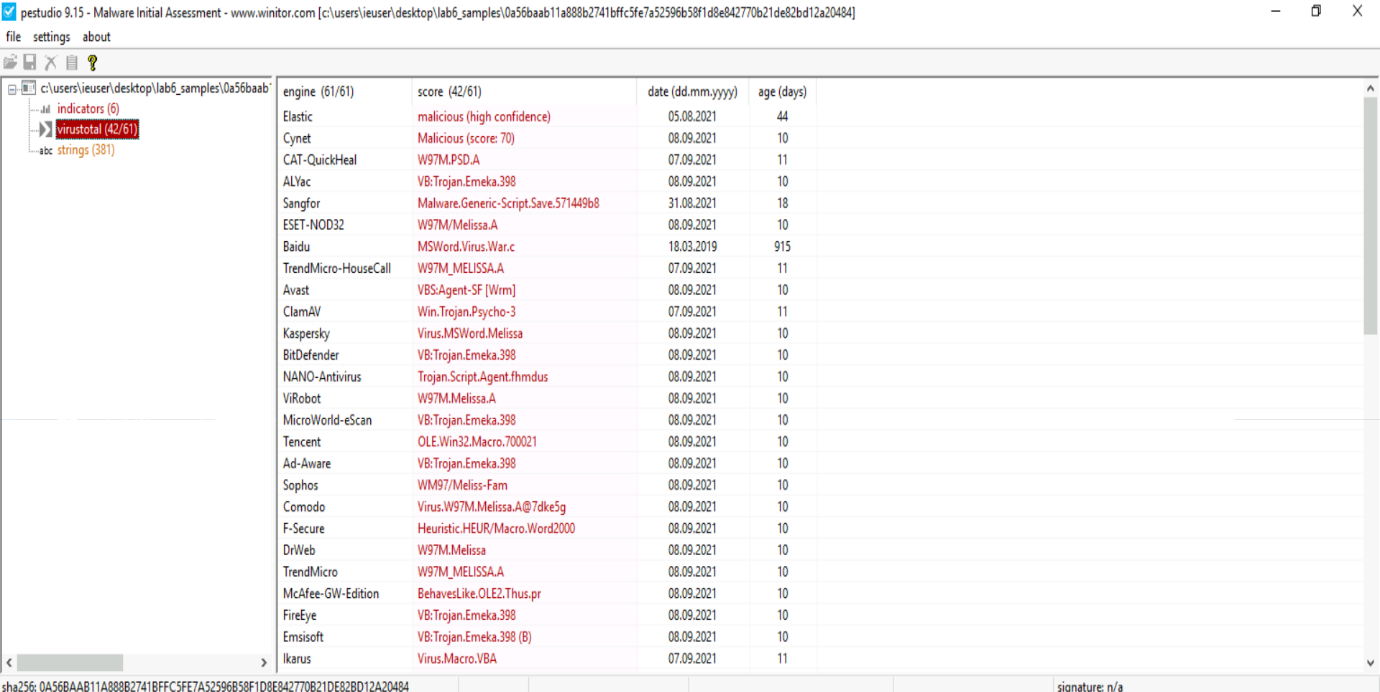
VirusTotal info in PEStudio

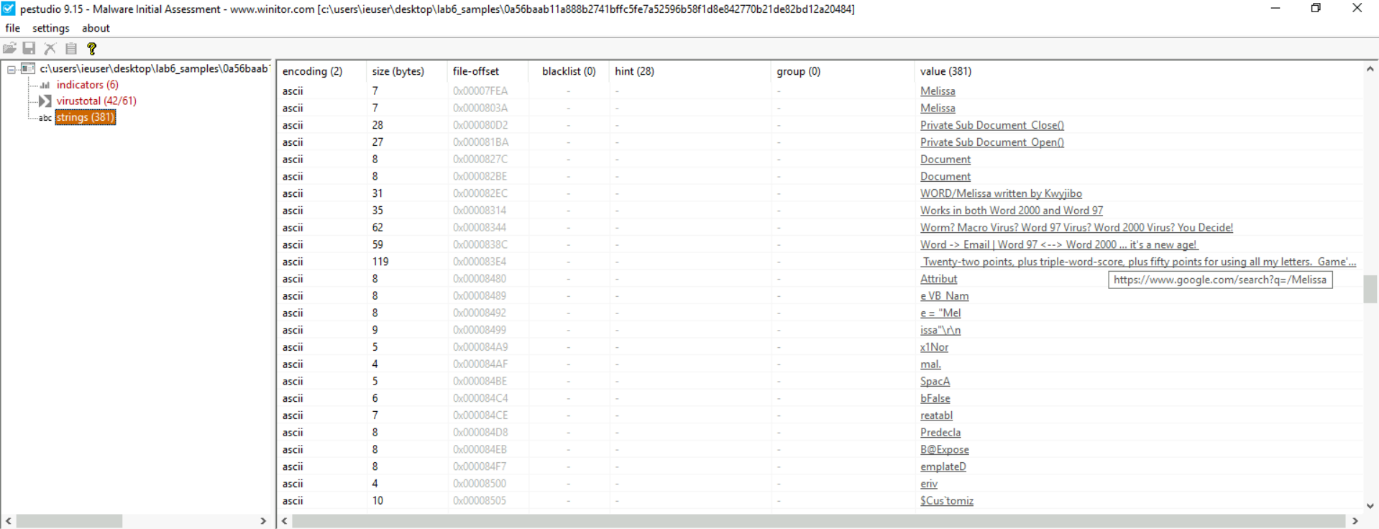


Strings in PEStudio



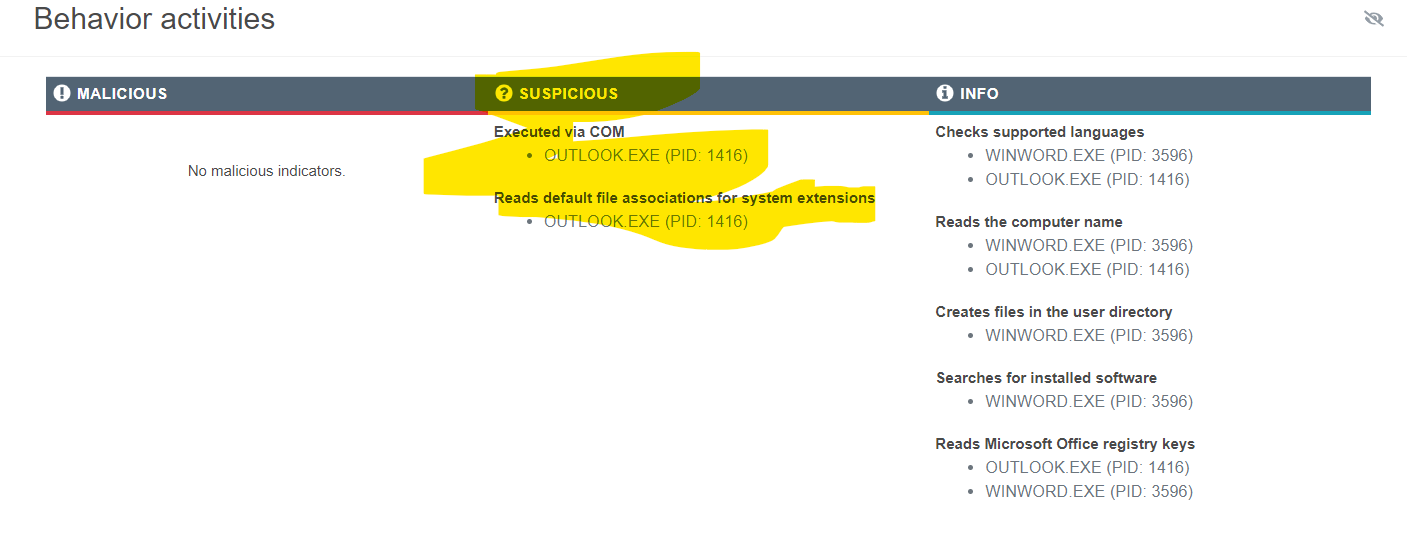


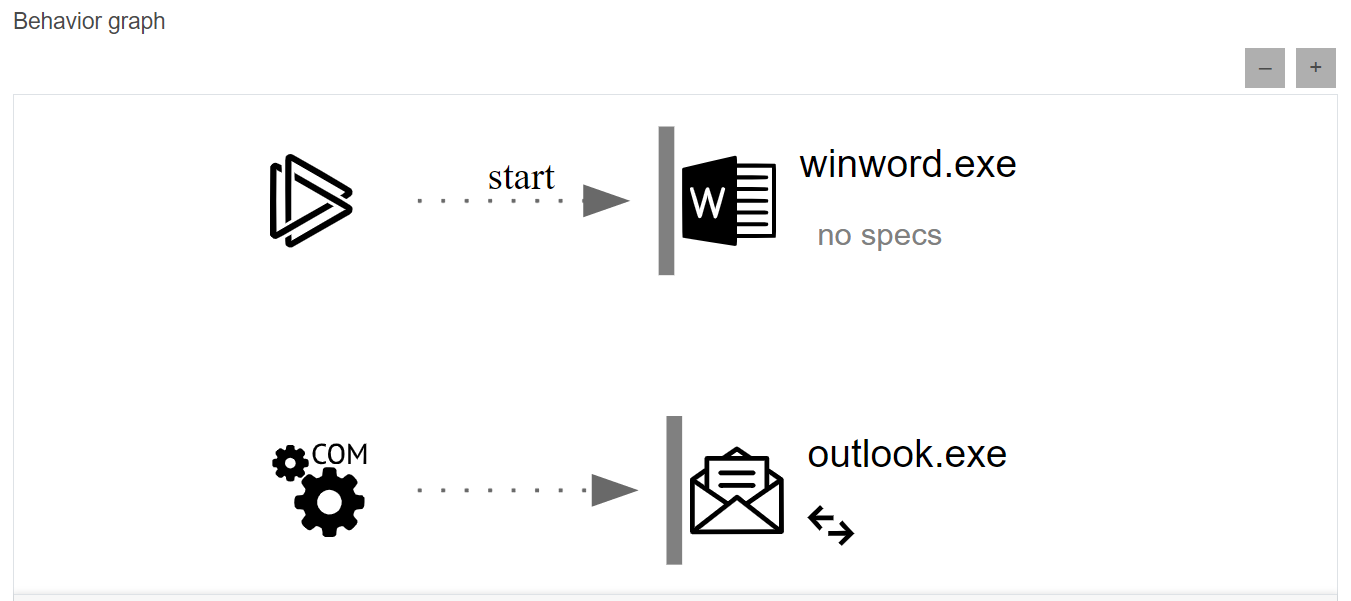


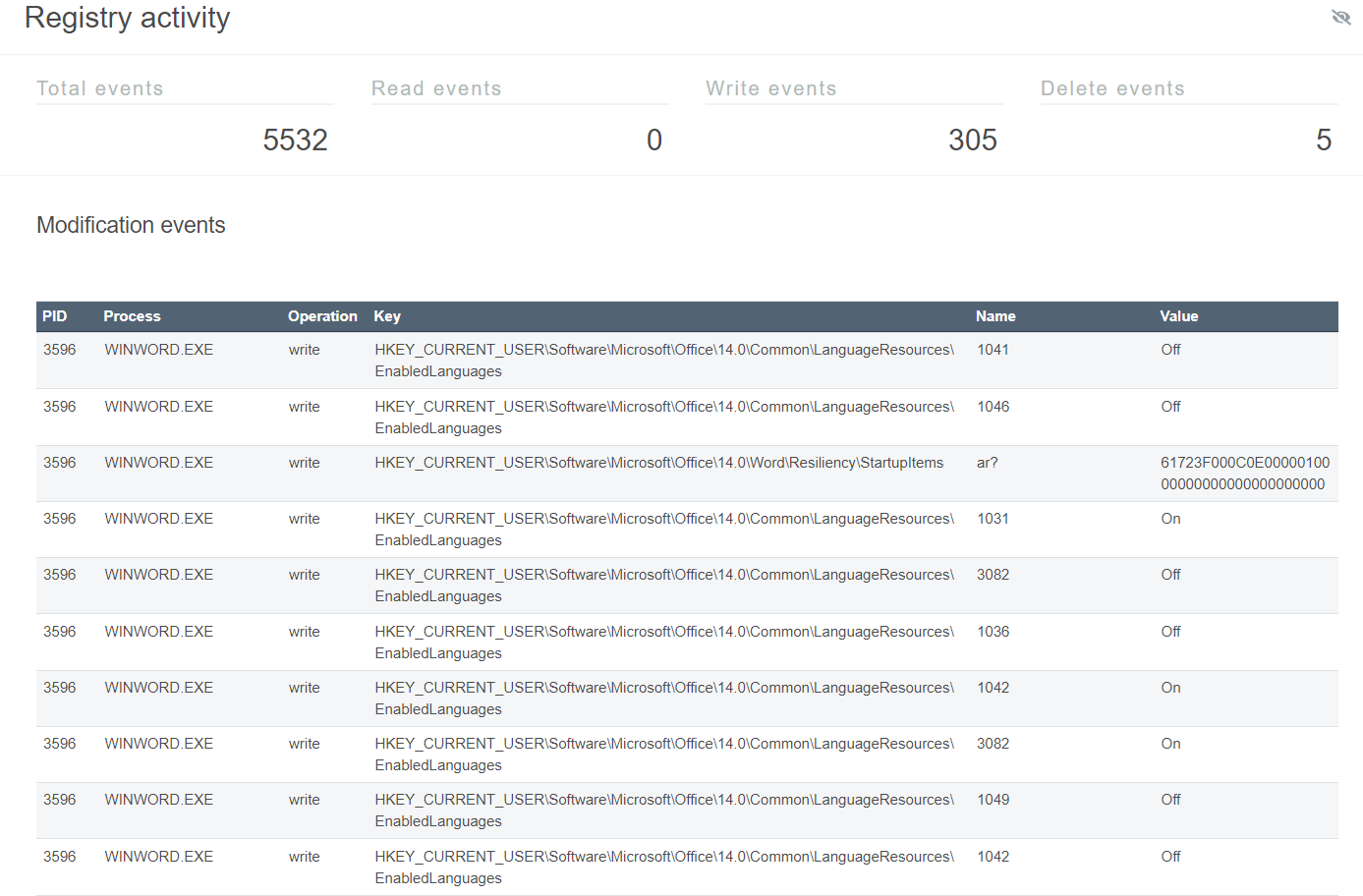


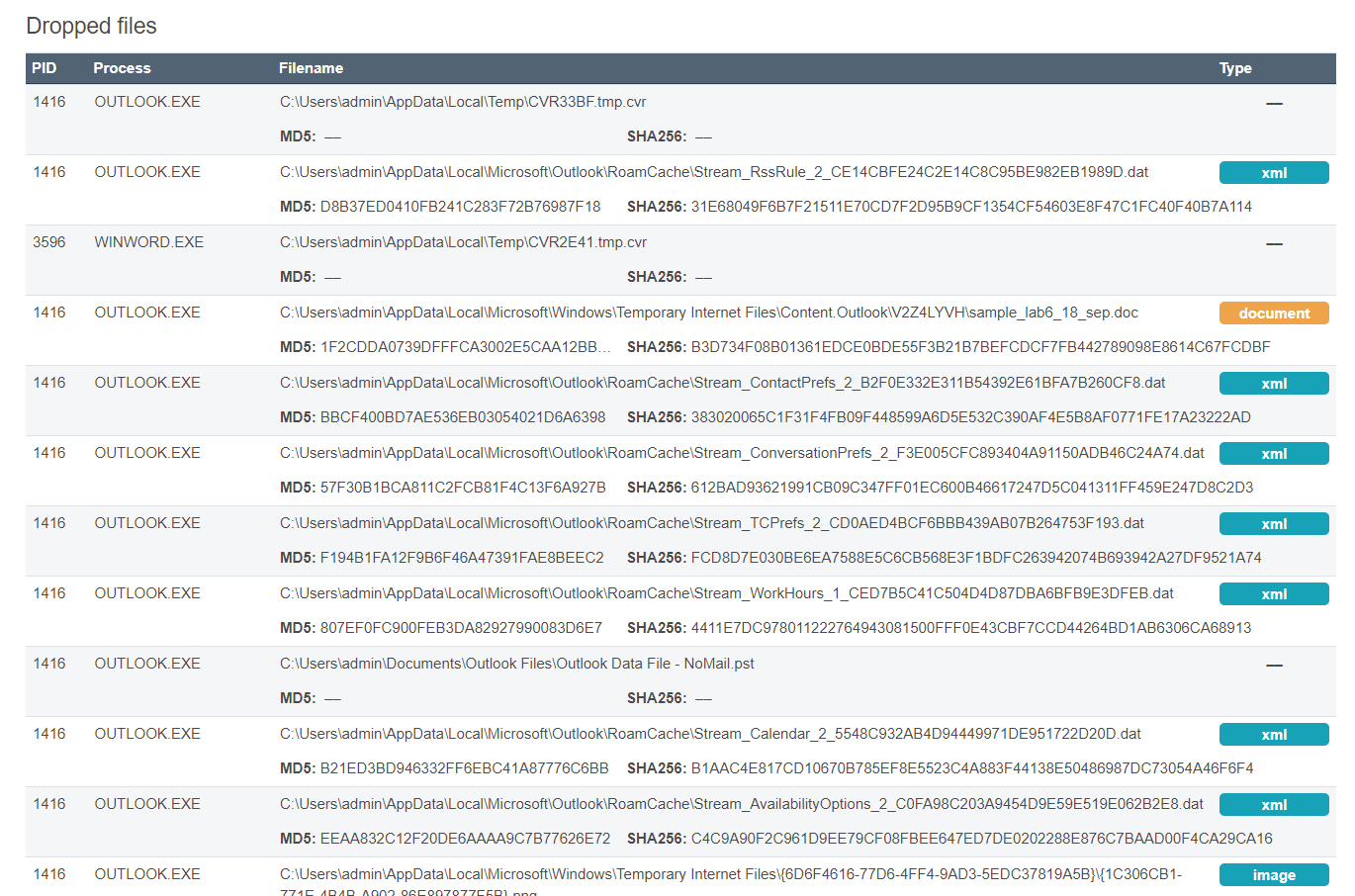
# Dynamic Analysis:

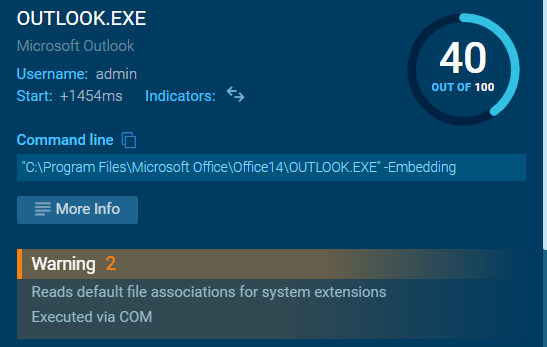
It was done in Any.run

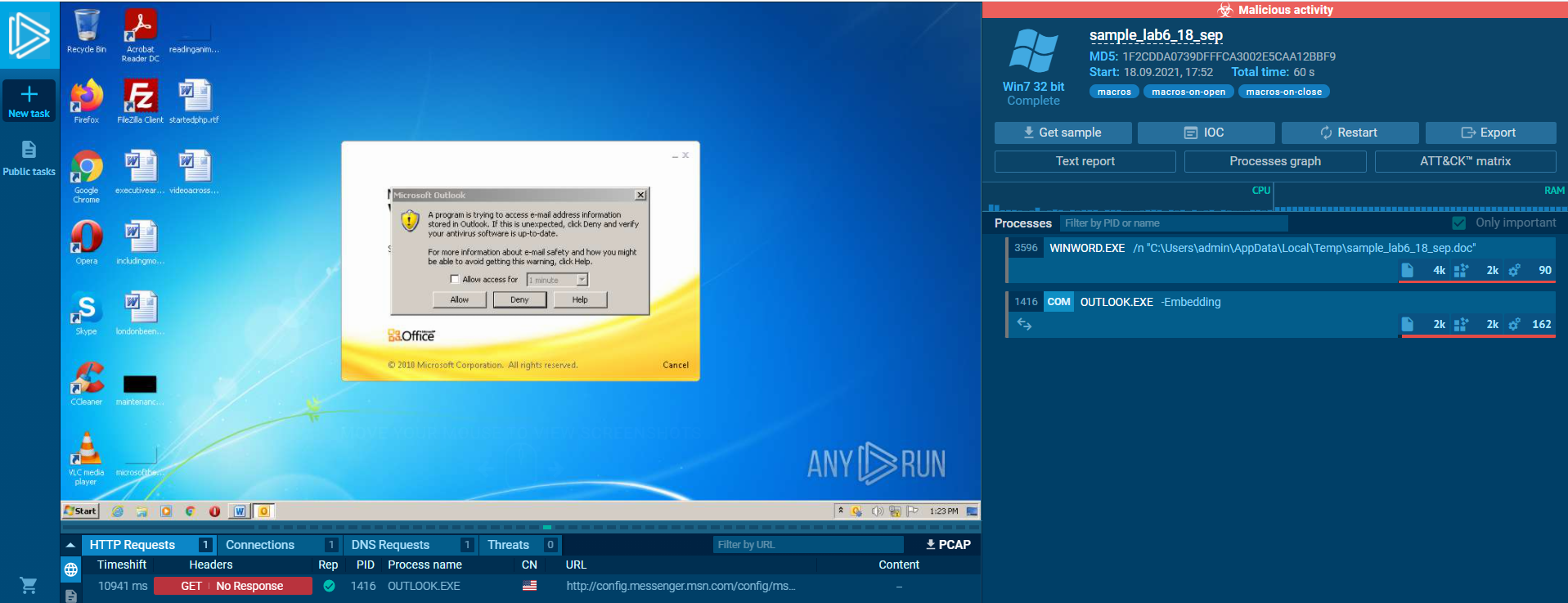












Below is the full run report link

<https://any.run/report/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf/bd809867-0318-450d-a33a-5de77f90d721>

# Yara rule :



# Reference :

[1] - <https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519>

[2] - <https://searchsecurity.techtarget.com/definition/Melissa-virus>