# **Lab 6: Analyse the file: sample\_lab6\_18\_sep**

## **Type of file**

File in Hexed.it

A screenshot of a computer

Description automatically generated with medium confidence

File Signature database:

Table

Description automatically generated

Type of File: **MS Office Document.**

## **Static analysis**

File in PE Studio:

Melissa Virus

Graphical user interface, application, table

Description automatically generated

Table

Description automatically generated

Olevba:

Text

Description automatically generated

Olevba output:

Graphical user interface, text, application, email

Description automatically generated

## **What file do?**

From olevba macro code analysis of the file with Melissa Virus.

Graphical user interface, text, application

Description automatically generated

When the file is opened the macro code will disable the MS Word security.

Graphical user interface, text, application

Description automatically generated

Then logs into the client’s outlook application and send mails to all the contacts in the address list, with Subject and Message body as highlighted above, with the current document attached.

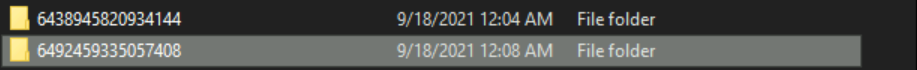
## **Threat intel**

Virus Total: Different names in which this file was submitted

Graphical user interface, text, application, email

Description automatically generated

Other Files:



Details on Melissa:

* Fast Spreading macro virus, which was distributes as an email attachment.
* When opened, it disables the security in Word 97 and Word 2000.
* If the user has Outlook application mail is sent to first 50 addresses in the address book with this file as attachment.
* Melissa does not destroy other files or resources but disables the corporate and other mail servers as the email distribution becomes large.

## **Yara Rule**

rule search\_melissa

{

meta:

author = "Arjun Anil"

description = "To find files with Melissa virus"

strings:

$a = "Macros"

$b = "Melissa"

$c = "WORD/Melissa written by Kwyjibo"

condition:

$a and $b or $c

}

Output:

Text

Description automatically generated

With New Samples

A computer screen capture

Description automatically generated with low confidence

## **References**

1. <https://searchsecurity.techtarget.com/definition/Melissa-virus>
2. <https://filesignatures.net/index.php?page=all&currentpage=16&order=SIGNATURE>
3. <https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf/details>