**Threat Intelligence - Lab 6**

**Submitted By: Sarathkumar MC – MT20ACS531**

**Melissa Virus Analysis**

|  |  |  |
| --- | --- | --- |
| **Table of Contents** | | |
| **S.No** | **File Name** | **Page No** |
| 1 | Sample 1 - sample\_lab6\_18\_sep | 2 |
| 2 | Sample 2 - 6492459335057408.zip | 5 |
| 3 | Sample 3 - 5644464565682176 .zip | 8 |
| 4 | Yara rule | 10 |

**Sample 1**

|  |  |
| --- | --- |
| File Name | sample\_lab6\_18\_sep |
| SHA256 | b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf |
| VirusTotal | [https://www.virustotal.com/gui/file/ b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf](https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf) |
| Alienvault OTX | [https://otx.alienvault.com/indicator/file/ b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf](https://otx.alienvault.com/indicator/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf) |
| File Signature | Starts with “D0 CF” that corresponds to doc, xls, ppt, msg files by Microsoft |
| Malware Classification | W97M/Melissa.A, Virus.MSWord.Melissa |

Screenshots:

VirusTotal

Graphical user interface, application

Description automatically generated

OTX:

Graphical user interface, text, application

Description automatically generated

PE Studio:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application, table, Excel

Description automatically generated

OLEVBA

Text

Description automatically generated

VB Script extracted using olevba

Graphical user interface, text, application

Description automatically generated

**Sample 2**

|  |  |
| --- | --- |
| File Name | 6492459335057408.zip |
| SHA256 | 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484 |
| VirusTotal | [https://www.virustotal.com/gui/file/ 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484](https://www.virustotal.com/gui/file/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484) |
| Alienvault OTX | [https://otx.alienvault.com/indicator/file/ 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484](https://otx.alienvault.com/indicator/file/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484) |
| File Signature | Starts with “D0 CF” that corresponds to doc, xls, ppt, msg files by Microsoft |
| Malware Classification | W97M/Melissa.A, Virus.MSWord.Melissa |

Screensots

VirusTotal

Graphical user interface, application

Description automatically generated

OTX

Graphical user interface, application

Description automatically generated

PEStudioGraphical user interface, application, table

Description automatically generated

Olevba

Text

Description automatically generated

VB Script extracted from Sample

Graphical user interface, text, application

Description automatically generated

**Sample 2**

|  |  |
| --- | --- |
| File Name | 5644464565682176.zip |
| SHA256 | ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c |
| VirusTotal | [https://www.virustotal.com/gui/file/ ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c](https://www.virustotal.com/gui/file/ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c) |
| File Signature | Starts with “D0 CF” that corresponds to doc, xls, ppt, msg files by Microsoft |
| Malware Classification | W97M/Melissa.A, Virus.MSWord.Melissa |

Screensots

VirusTotal

<https://www.virustotal.com/gui/file/ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c>

Graphical user interface, application

Description automatically generated

PEStudio:

Graphical user interface, application

Description automatically generated

Olevba

Graphical user interface, text

Description automatically generated

VB Script Extracted from Malware Sample

Graphical user interface, text, application

Description automatically generated

**Yara Rule**

rule MicrosoftMelissa

{

meta:

description = "MicrosoftMelissa is a virus that speads over outlook"

os = "mswindows"

filetype = "Macro"

maltype = "Virus"

strings:

$melissa0 = "Important Message From"

$melissa1 = "Here is that document you asked for ... don't show anyone else ;-)"

$melissa2 = "WORD/Melissa written by Kwyjibo"

$melissa3 = "Works in both Word 2000 and Word 97"

$melissa4 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"

$melissa5 = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"

condition:

all of ($melissa\*)

}

Yara Rules

Text

Description automatically generated

Output

Text

Description automatically generated

**Conclusion:**

Thus, Yara rules have been identified and written for the given malwares and it is able to find and filter out the Melissa infected files.